

KYMENLAAKSON AMMATTIKORKEAKOULU

Tietotekniikka / Tietoverkkotekniikka

Tuire Nuutinen

LANGATON LÄHIVERKKO JA SEN HALLINTA

Opinnäytetyö 2015

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU

tietotekniikka

NUUTINEN, TUIRE

Langaton lähiverkko ja sen hallinta

Opinnäytetyö

40 sivua + 6 liitesivua

Työn ohjaaja

Martti Kettunen, yliopettaja

Toimeksiantaja

Kymenlaakson ammattikorkeakoulu

Huhtikuu 2015

Avainsanat

802.11, Cisco Prime Network Control System,
SDLC, WLAN, WLAN-kontrolleri

Tämän tutkimuksen aiheena on langaton lähiverkko ja sen hallinta ja tavoitteena oli rakentaa yrityksen informaatioteknologian osastolle uusi, toimivampi ja käyttäjäystävällisempi langaton lähiverkko. Tutkimuksen menetelminä oli tutustuminen alan kirjallisuuteen sekä käytännön työnä langattoman lähiverkon laitteiden asentaminen ja konfiguroiminen.

Työssä perehdytään langattoman verkon 802.11-standardeihin sekä MIMO- ja roaming-tekniikoihin, joita työssä rakennetun lähiverkon laitteissa on hyödynnetty. Tutkimuksessa käydään lyhyesti läpi, mitä laitteita langattomassa lähiverkossa voi olla sekä kerrotaan tarkemmin, mitkä laitteet juuri tässä työssä on otettu käyttöön ja niiden ominaisuuksista. Työssä kerrottiin lyhyesti myös Cisco Prime Network Control System -hallintaohjelmasta, jolla langatonta lähiverkkoa on tarkoitus jatkossa hallita. Yhtenä osa-alueena on järjestelmien kehittämisen elinkaari, jonka mukaisissa vaiheissa käytännön työssä on edetty.

Työssä rakennettu langaton lähiverkko koostuu yhdestä Cisco 2500 -sarjan kontrollerista, yhdestä Power over Ethernet -kytkimestä sekä kahdeksasta Cisco Aironet 3700 -sarjan tukiasemasta. Kontrollerilla hallinnoidaan tukiasemia, jotta niitä ei tarvitse konfiguroida yksitellen, mikä yksinkertaistaa verkon hallintaa. Tukiasemat on kytketty PoE-kytkimeen, jonka kautta ne saavat virran, eivätkä ne tällöin tarvitse erillisiä virtajohtoja.

Työn tavoitteissa onnistuttiin hyvin, koska uusi langaton lähiverkko rakennettiin ja sen käyttäjäystävällisyyttä parannettiin entiseen verrattuna sillä, että verkkoon kirjaudutaan omilla tunnuksilla.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU

University of Applied Sciences

Information Technology

NUUTINEN, TUIRE

Bachelor's Thesis

Supervisor

Commissioned by

April 2015

Keywords

Management of Wireless Local Area Network

40 pages + 6 pages of appendices

Martti Kettunen, Principal Lecturer

Kymenlaakso University of Applied Sciences

802.11, Cisco Prime Network Control System,
SDLC, WLAN, Wireless LAN controller

The topic of this study is management of wireless local area network and the objective was to build a new, more functional and user-friendly wireless local area network for company's department of information technology. The methods of this study consist of becoming acquainted with literature of the field and installing and configuring the required devices.

The study describes 802.11 standards of the wireless local area network and MIMO and roaming techniques which were used in the devices. This study briefly describes what kind of devices can be installed in a wireless local area network and more specifically what devices were used in this study. The wireless local area network built for the study will be managed in the future with Cisco Prime Network Control System which is also described in the thesis. One aspect of the study is system development life cycle because planning and building the wireless local area network follows the phases of it.

The wireless local area network built for this study consist of one Cisco 2500 series wireless LAN controller, one Power over Ethernet switch and eight Cisco Aironet 3700 series access points. The access points are managed from the controller so one do not have to configure them individually. The access points are connected to the PoE switch from which they gain power so they do not need separate power cords.

The work objectives were met well because the new wireless local area network was built and it is more user-friendly because clients uses own identifiers to sign in to the network.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

SANASTO JA LYHENTEET	6
1 JOHDANTO	8
1.1 Kymenlaakson ammattikorkeakoulu	8
1.2 KyAMK Informaatioteknologia	8
2 STANDARDIT JA TEKNIIKAT	10
2.1 802.11a ja 802.11b	11
2.2 802.11g	11
2.3 802.11n	12
2.4 802.11ac	12
2.5 MIMO-tekniikka	12
2.6 Roaming	13
3 LANGATON LÄHIVERKKO	16
3.1 Cisco 2500 WLAN-kontrolleri	17
3.2 Cisco Aironet 3700 tukiasema	17
3.3 Cisco Prime Network Control System	18
4 JÄRJESTELMIEN KEHITTÄMISEN ELINKAARI	19
4.1 Mallisuunnittelu	19
4.2 Rakentaminen	19
4.3 Testaus	20
4.4 Käyttöönotto	20
4.5 Big Bang -malli	21
5 TYÖN TOTEUTUS	21
5.1 Projektiopinnot	22
5.2 Uusi WLAN-kontrolleri	23
5.2.1 Liitännät	24

5.2.2 Eri WLANit asiakkaille ja vierailijoille	25
5.2.2.1 WLAN Kalaverkko	26
5.2.2.2 WLAN Vieraskala	27
5.2.3 CleanAir	28
5.3 Langattomat tukiasemat	30
5.4 Power over Ethernet -kytkin	30
5.5 Palomuuuri	31
5.6 Hallintaohjelma Cisco Prime NCS	32
6 LOPPUPÄÄTELMÄT	36
LIITTEET	

Liite 1. Kytkimen konfiguraatiot

SANASTO JA LYHENTEET

AAA-protokolla	Authentication, authorization and accounting: <i>käyttäjän tunnistaminen (autentikointi), käyttäjän valtuutus tehdä tiettyjä asioita (valtuutus) ja käyttäjien tilastotietojen keräys (tilastointi)</i>
AP	access point: <i>tukiasema, laite, joka toimii verkon lähettimenä ja vastaanottimena</i>
DHCP	Dynamic Host Configuration Protocol: <i>verkkoprotokolla, jonka yleisin tehtävä on jakaa lähiverkkoon kytkeytyville laitteille IP-osoite</i>
DHCP-pool	<i>DHCP:seen määritetty IP-osoiteavaruus, josta asiakkaille jaetaan IP-osoitteet</i>
IEEE	The Institute of Electrical and Electronics Engineers: <i>kansainvälinen tekniikan alan järjestö</i>
LAN	local area network: <i>lähiverkko</i>
MIMO	multiple-input, multiple-output: <i>tietoliikennetekniikka, jossa tiedonsiirrossa käytetään samanaikaisesti useampaa kuin yhtä antennia</i>
NAT	Network Address Translation: <i>osoitteenmuunnos, tekniikka, joka mahdollistaa sen, että useampi laite saa yhteyden internetiin, vaikka niillä olisi käytössä vain yksi uniikki IP-osoite</i>
RADIUS	Remote Authentication Dial In User Service: <i>verkkoprotokolla, joka tarjoaa AAA-protokollan käytön</i>

SISO	single-in, single-out: <i>tietoliiketekniikka, jossa tiedonsiirrossa käytetään vain yhtä lähettävää ja yhtä vastaanottavaa antennia</i>
spatial stream	<i>tiedonsiirtotekniikka, jossa useampi antenni käyttää samanaikaisesta samalla radiotaajuudella eri avaruudellisia tiloja</i>
SSH	Secure Shell: <i>salattuun tietoliikeneeseen tarkoitettu yhteydenottoprotokolla</i>
Telnet	<i>yhteydenottoprotokolla, jonka kautta kulkevaa tietoliikennettä ei salata lainkaan</i>
WLAN	wireless local area network: <i>langaton lähiverkko</i>

Tämän opinnäytetyön tarkoituksena on rakentaa uusi, luotettavampi ja käyttäjäystävällisempi langaton lähiverkko yrityksen informaatioteknologian osastolle. Työssä on tarkoitus myös asentaa ja hallinnoida rakennettua lähiverkkoa Cisco Prime Network System Control -ohjelmistolla, mutta ohjelmiston asennuksen viivästyessä sitä ei lisätä enää tähän opinnäytetyöhön.

1.1 Kymenlaakson ammattikorkeakoulu

Kymenlaakson ammattikorkeakoulu tarjoaa korkeakoulututkintoja niin päivä- kuin monimuoto-opintoina, minkä lisäksi siellä voi suorittaa myös ylemmän ammattikorkeakoulun, ja avoimenkin AMK:n kurseja on tarjolla. Korkeakoulussa voi opiskella joitakin aloja myös englannin kielellä. Kymenlaakson ammattikorkeakoulun toimipisteet ovat Kouvolassa Kasarminmäellä ja Kotkassa Metsolassa. (Kymenlaakson ammattikorkeakoulu 2015.)

Kymenlaakson ammattikorkeakoulu on osana uutta Kaakkois-Suomen korkeakoulurakennetta erikoistuen yhteistyöhön Venäjän kanssa sekä osaamiseen EU-Kymenlaakso-Venäjä-akselilla. Kymenlaakson ammattikorkeakoulu painottaa tehtävässään alueen elinkeinorakennetta uudistavaan koulutukseen sekä tutkimus- ja kehittämistoimintaan. Kyamkin painoaloja ovat ympäristöystävällinen energiantuotanto ja sen hyödyntäminen, kilpailukykyinen logistiikka ja merenkulku sekä hyvinvointi- ja liiketoimintapalvelut. (Kymenlaakson ammattikorkeakoulu 2014.)

1.2 KyAMK Informaatioteknologia

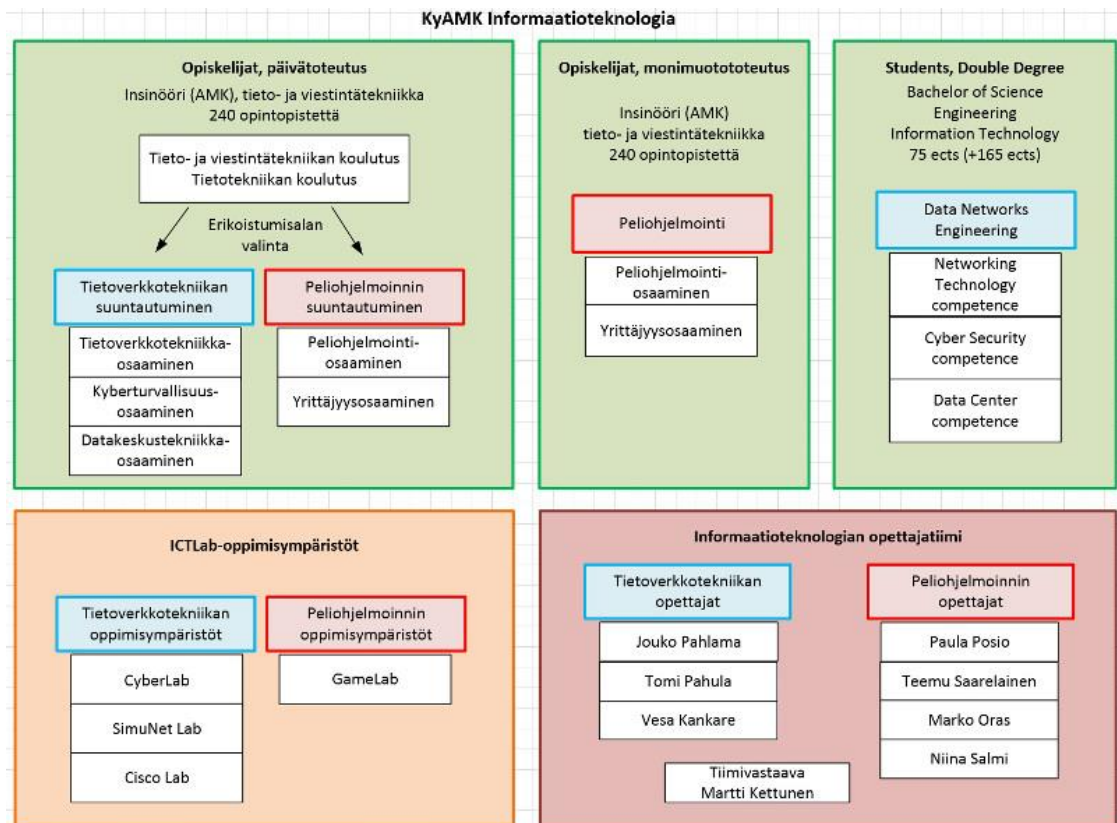
Työ toteutettiin Kymenlaakson ammattikorkeakoulun Informaatioteknologialle, jonka tiloihin työssä rakennettu langaton lähiverkko tehtiin. KyAMK Informaatioteknologia koostuu Kymenlaakson ammattikorkeakoulun tieto- ja viestintätekniikan opiskelijoista, ICTLab-oppimisympäristöistä sekä Informaatioteknologian opettajatiimistä. (KyAMK Informaatioteknologia 2015a).

Tieto- ja viestintätekniikan opiskelija valitsee ensimmäisen opiskeluvuotensa aikana erikoistumisalan eli suuntautuu joko tietoverkkotekniikkaan tai peliohjelmointiin. Tietoverkkotekniikan suuntautuminen pitää sisällään sysventävän tietoverkkotekniikan osaamisalueen lisäksi kyberturvallisuuden ja datakeskustekniikan osaamisalueet. Peliohjelmoinnin suuntautuminen mahdollistaa peliohjelmoinnin osaamisalueen lisäksi yrittäjyysosaamisen opiskelun. (KyAMK Informaatioteknologia 2015a.)

Tietoverkkotekniikan oppimisympäristö jakautuu kolmeen osioon, joista Cisco Lab antaa mahdollisuuden käytännönläheiseen opetukseen tarjoamalla tarvittavia verkkolaitteita, kuten reitittimiä, kytkimiä ja palomuuria opetuksen tueksi. Toinen osio on SimuNet-hankkeen operaattoritasoinen tuotantoverkko SimuNet Lab, joka on jatkuvasti ”tuotannossa”. Tästä tuotantoverkosta löytyy kaikki tärkeimmät palvelut, joita oikeatkin verkkopalveluntarjoajat myyvät yrityksille. Kolmas osio on CyberLab, jossa voidaan opiskella datakeskusten ja erilaisten tietoverkkojen sekä järjestelmien tietoturvallista toteuttamista, penetraatiotestauksia ja tunkeutumisen havaitsemista. Osa CyberLabin tarjoamista opetuksista toteutetaan myös pelien keinoin. (KyAMK Informaatioteknologia 2015b.) (KyAMK Informaatioteknologia 2015c.)

KyAMK Informaatioteknologian Peliohjelmointi-sivulla kerrotaan, että ”*opinnoissa perehdytään pelialan ohjelmistotuotantoon ja peliohjelmointiin, mutta koulutus antaa valmiudet toimia missä tahansa ohjelmistotekniikan sovellusalueella.*” (KyAMK Informaatioteknologia 2015d.) Peliohjelmoinnin suuntautumisen suorittaneet opiskelijat työllistyvätkin erilaisiin ohjelmistotaloihin tai muihin pelialan yrityksiin, joissa he voivat toimia asiantuntijatehtävissä tietojärjestelmien, dynaamisten verkkopalveluiden ja ohjelmistojen parissa (KyAMK Informaatioteknologia 2015d).

Kuvassa 1 on havainnoillistettu KyAMK Informaatioteknologian rakenne.



Kuva 1: KyAMK Informaatioteknologia (kuvan lähde KyAMK Informaatioteknologia. 2015a)

2 STANDARDIT JA TEKNIIKAT

Useimmiten langattomalla lähiverkolla (WLAN) tarkoitetaan IEEE:n luomaa 802.11-määritelmäperhettä, mutta langattomia lähiverkkoja on muitakin, esimerkiksi European Telecommunications Standards Instituten luoma Hiperlan (Rube 2015). Toinen yleistys on puhua Wi-Fistä tarkoittaessa langatonta verkkoyhteyttä, mikä sekin on virheellinen olettaus. Wi-Fi on *Wi-Fi Alliancen* tavaramerkki, jolla järjestö merkitsee tuotteet Wi-Fi-yhteensopiviksi. Tällä merkillä varustetut laitteet on tutkittu ja testattu niin, että ne toimivat kaikkien muiden Wi-Fi-merkillä varustettujen laitteiden kanssa. (Grandlund 2007, 293.) (Wi-Fi Alliance 2015.)

Tässä työssä WLANilla tarkoitetaan nimenomaan IEEE:n 802.11-määritelmäperhettä, joka pitää sisällään useita eri versioita. Ensimmäinen versio, vuonna 1997 hyväksytty 802.11 tarjosi ainoastaan 1 - 2 Mbps:n datasiirtonopeuden 2.4 Ghz:n taajuudella, mikä

on selkeästi hitaampi kuin aikaisemmin julkaistu kaapelilla toimiva Ethernet 100Base-x-ratkaisu, jonka teoreettinen nopeus on 100 Mbps. (Grandlund 2007, 284, 294.) (Penttinen 2006, 115.)

2.1 802.11a ja 802.11b

Vuonna 1999 julkaistiin kaksi uutta versiota, 802.11a ja 802.11b. Jälkimmäinen toimi alkuperäisen standardin tapaan 2.4 GHz:n taajuudella, jolloin tuotekustannukset pysyivät alhaisina, minkä lisäksi signaalin kantomatko ja esteettömyys oli hyvä. Mutta myös datasiirtonopeus pysyi alhaisena. Teoreettinen maksiminopeus 802.11b-standardilla on 11 Mbps. Lisäksi kodinkoneet, esimerkiksi mikroaaltouunit toimivat samalla taajuudeella, joten ne saattavat aiheuttaa häiriötä, jos laitteita käyttää liian lähellä toisiaan. (Grandlund 2007, 294.) (Mitchell 2015.)

802.11a-standardi tarjoaa teoreettisesti jopa 54 Mbps:n datasiirron, koska se käyttää 5 GHz:n taajuutta. Korkeamman taajuuden käyttäminen kuitenkin lyhentää signaalin kantomatkaa sekä heikentää sen kykyä läpäistä seiniä ja muita esteitä. Lisäksi 802.11a-standardin tuotantokustannukset olivat korkeammat, minkä takia se ei saanut yhtä suurta suosiota kuin 802.11b. Tämän myötä 802.11a-standardia käytettiin enemmän yritysverkoissa, kun taas 802.11b oli suosittu kotikäytössä. (Mitchell 2015.) (Puska 2005, 45-46.)

2.2 802.11g

Kesäkuussa 2003 hyväksyttiin uusi standardi, joka periaatteessa yhdistää kahden edeltävän standardin hyvät puolet. 802.11g on periaatteessa sama kuin 802.11a, mutta se toimii 2.4 GHz:n taajuudella. Tämän ansiosta 802.11g:n ja 802.11b:n mukaisia laitteita voidaan käyttää keskenään, mutta 802.11g:n teoreettisen maksiminopeus 54 Mbps on mahdollista ainoastaan silloin, kun kaikki verkon laitteet tukevat sen mukaista standardia. Jos verkossa on siis yksikin 802.11b:n mukainen laite, on verkon nopeus kyseisen standardin mukaista eli enintään 11 Mbps. (Grandlund 2007, 305)

2.3 802.11n

802.11n-standardin uutena ominaisuutena on MIMO-tekniikka, jossa käytetään hyväksi useampaa lähettävää ja vastaanottavaa antennia. Tämän ansiosta 802.11n-standardin teoreettinen nopeus on jopa 600 Mbps, mutta käytännössä nopeudeksi luvataan noin 140 Mbps. 802.11n-standardin toisena uutena ominaisuutena on myös se, että se toimii niin 2,4 kuin 5 GHz:n taajuudella. (Hucaby 2014, 55-56.)

802.11n on yhteensopiva 802.11a/b/g-standardien kanssa, minkä lisäksi uuden Cisco ClientLink -teknologian ansiosta vanhemman version mukaiset laitteet eivät hidasta koko verkon toimintaa. Tämän ansiosta 802.11n-version käyttöönotto ei estä käyttämästä vanhempien version mukaisia laitteita pidentäen niiden käyttöikää. (Grandlund 2007, 305.) (Cisco Systems 2009.)

2.4 802.11ac

Tässä työssä rakennetun lähiverkon kaikki laitteet tukevat tällä hetkellä uusinta langatonta lähiverkkostandardia 802.11ac:ta, joka hyväksyttiin 7.1.2014. Tämän on tarkoitettu parantavan langattoman lähiverkon käyttöä tarjoamalla jopa 7 Gbps datasiirtonopeuden 5 GHz:n taajuudeella. Uusi standardi parantaa myös varsinkin älypuhelin- ja taulutietokoneasiakkaiden langattoman lähiverkon käyttöä, koska standardi esittelee vallankumouksellisen uuden teknologian, joka tukee useita samanaikaisia alalinkkilähetystyksiä. Tällöin laitteissa, joissa on vähemmän lähettäviä ja vastaanottavia antennia (MIMO-tekniikka), voidaan silti parantaa datan siirtoa useamman spatiaalisen streamin ansiosta. (Kelly 2015.)

2.5 MIMO-tekniikka

MIMO (multiple-input, multiple-output) on tietoliikennetekniikka, jossa tiedonsiirrossa käytetään samanaikaisesti useampaa kuin yhtä antennia. Tällä tekniikalla voidaan joko parantaa tiedonsiirtonopeutta tai tiedonsiirron luotettavuutta. (Rohde & Schwarz GmbH & Co. KG 2015, 4.)

Kun tiedonsiirron molemmilla osapuolilla on vähintään yhtä monta antennia käytössään, voidaan jokaisen lähettäjä-vastaanottaja-antenniparin kautta lähettää yksilöllinen signaali. Teoriassa siirrettävän tiedon määrä moninkertaistuu antenniparien lukumäärän mukaisesti, mutta käytännössä useamman antennin samanaikainen käyttö aiheuttaa häiriöitä eikä tiedonsiirtomäärä ole suoraan verrattavissa antenniparien lukumäärään. (Rohde & Schwarz GmbH & Co. KG 2015, 4-6.)

Jos halutaan parantaa tiedonsiirron luotettavuutta, lähetetään useammasta antennista sama signaali. Tällöin viiveestä tai muista tiedonsiirrossa aiheutuvista häiriöistä ei ole samanlaista ongelmaa kuin, jos tieto lähetettäisiin vain yhdestä antennista. (Rohde & Schwarz GmbH & Co. KG 2015, 4-6.)

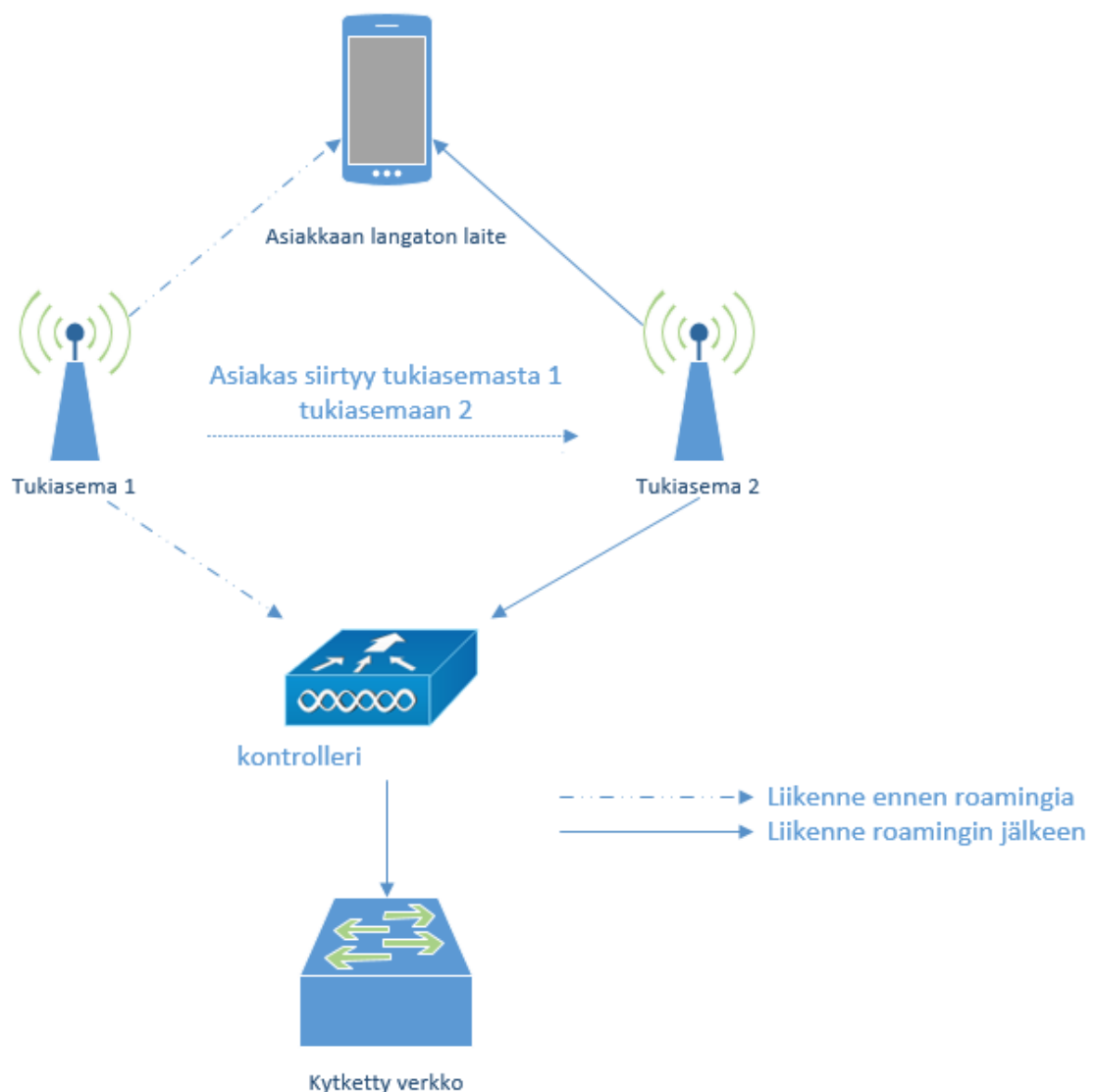
Laitteen käyttämien vastaanottavien ja lähettävien antennien lukumäärät merkitään $L \times V$ muodossa, jossa L on lähettävien ja V vastaanottavien antennien lukumäärä. Esimerkiksi 2×3 MIMO tarkoittaa, että laitteessa on kaksi lähettävää ja kolme vastaanottavaa antennia. (Hucaby 2014, 56.)

MIMO-tekniikan käyttäminen ei kuitenkaan vaadi, että yhteyden muodostavissa laitteissa olisi saman verran lähettäviä ja vastaanottavia antennia. Esimerkiksi tässä työssä käytettävissä tukiasemissa on 4×4 antennia, mutta siihen voidaan hyvin yhdistää laite, jossa on esimerkiksi 1×2 antennia. (Smith, Woodhams & Marg 2010, 51.)

2.6 Roaming

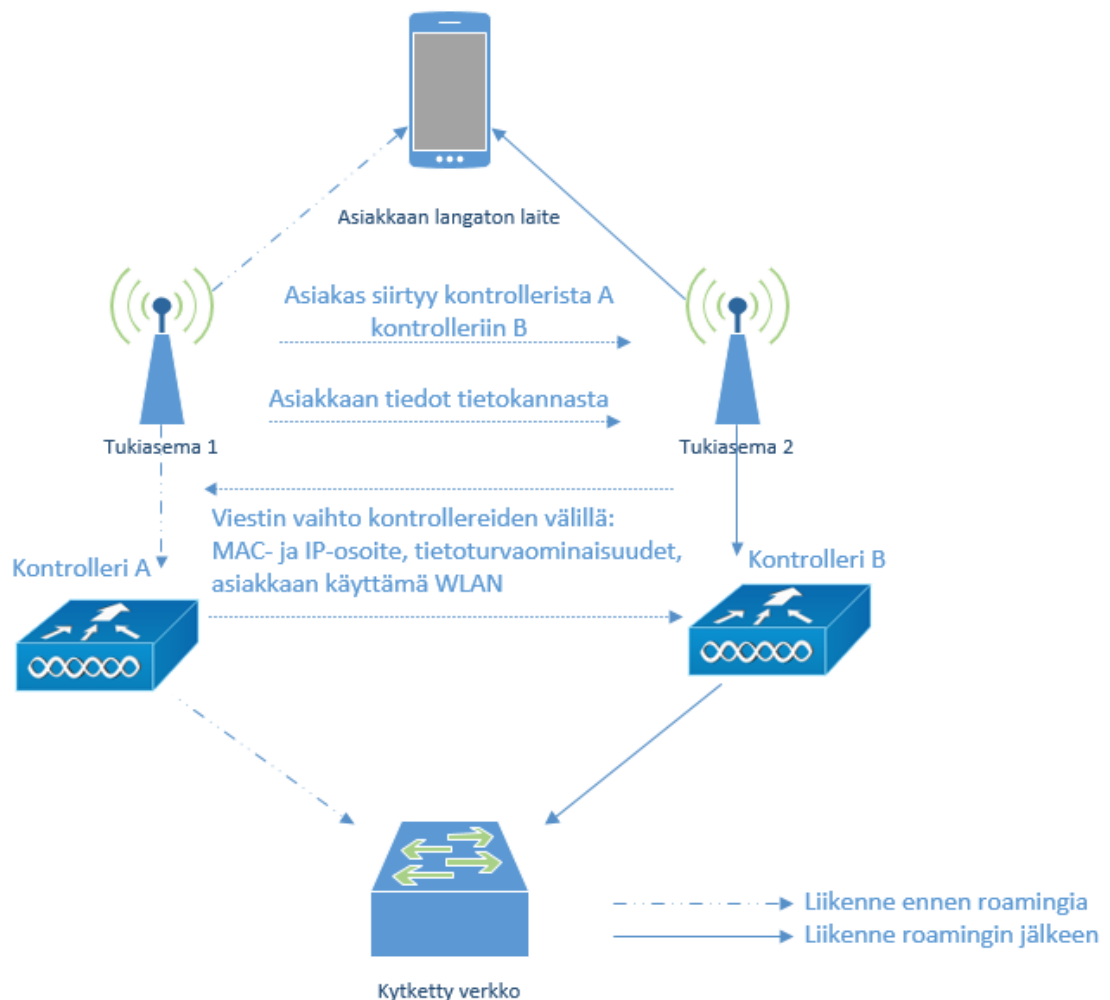
Roaming tarkoittaa sitä, että asiakas liikkuu esimerkiksi yrityksen tiloissa ja hänen langaton laitteensa siirtyy yrityksen lähiverkon tukiasemasta tai kontrollerista toiseen. Tällä pyritään tarjoamaan asiakkaan käyttöön paras mahdollinen yhteys, mutta roaming voi aiheuttaa myös käyttökatkoksia. Jos langaton lähiverkko on suojattu salasanalla, täytyy asiakkaan todentaa käyttöoikeutensa uudelleen siirtyessään tukiasemasta toiseen. (What-when-how 2015.)

Cisco Unified Mobilityn ansiosta asiakkaan ei tarvitse tunnistaudua uudelleen siirtyessään tukiasemasta tai kontrollerista toiseen, koska lähiverkon kontrolleri toimii tietokantana, johon tallennetaan asiakkaan tarvittavat tiedot. Näitä tietoja ovat esimerkiksi WLAN, jossa asiakas on, hänen laitteen IP- ja MAC-osoite, tukiasema, johon asiakas liittyi sekä tietoturvan ominaisuudet, kuten mitä asiakas saa tai ei saa tehdä verkossa. Jos asiakas siirtyy saman kontrollerin alla olevasta tukiasemasta toiseen (intra-controller roaming), ei kontrollerin tarvitse luoda kokonaan uutta asiakasta tietokantaan. Kontrollerin tarvitsee ainoastaan päivittää asiakkaan tietoihin käytettyä tukiasemaa koskeva tieto sekä mahdollisesti päivittää asiakkaan tietoturvaominaisuudet. Kuvassa 2 on kuvattu mitä intra-controller roamingissa tapahtuu. (What-when-how 2015.)



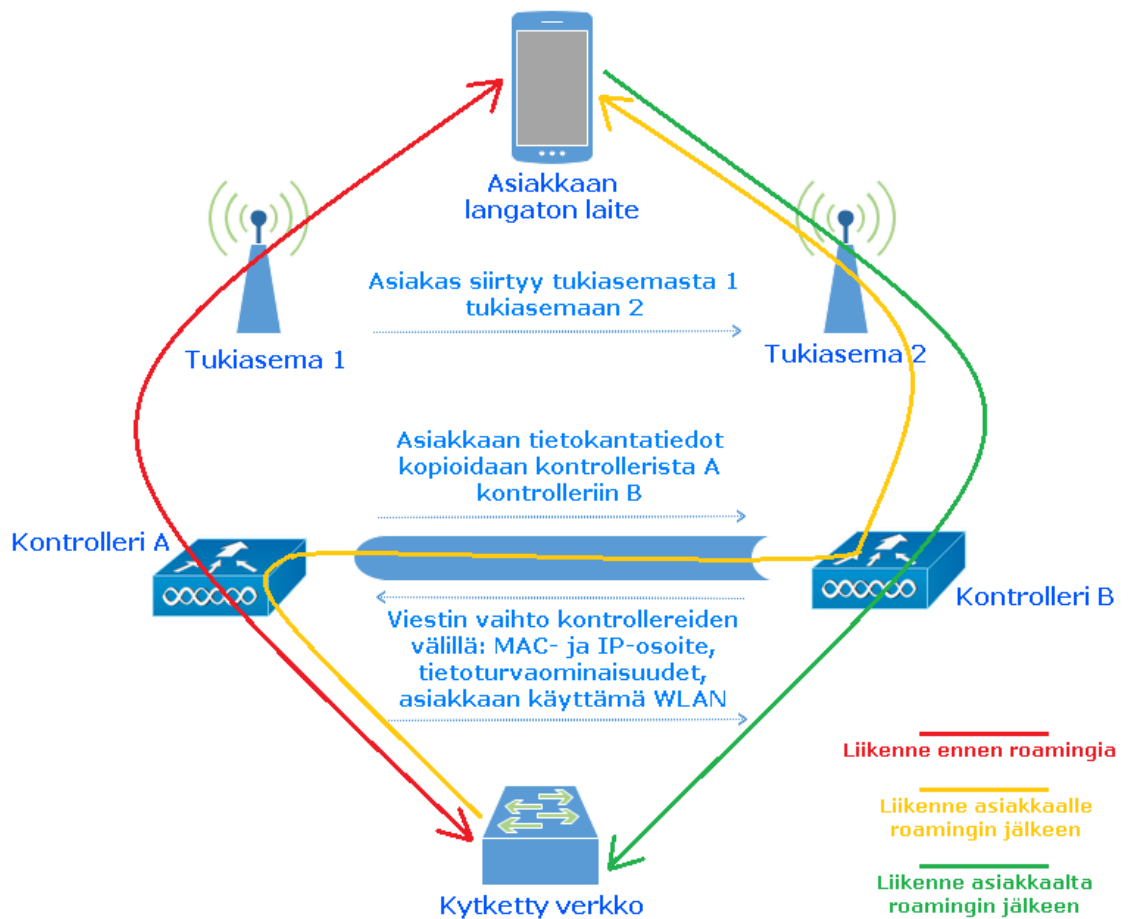
Kuva 2: Intra-controller roaming (What-when-how 2015)

Inter-controller roamingissa asiakas siirtyy eri kontrollerin alaisuudessa olevien tukiasemien välillä. Tällöin kontrollerit vaihtavat keskenään viestejä ja asiakkaan tietokantatiedot siirretään alkuperäisestä kontrollerista uuteen. Kuvassa 3 on havainnoillistettu inter-controller roamingin tapahtumat. (What-when-how 2015.)



Kuva 3: Inter-controller roaming (Whan-when-how 2015)

Lisäksi on myös inter-subnet roaming eli layer 3 roaming, joka tapahtuu, kun asiakas on alun perin kontrolleri A:ssa käyttäen VLANia X ja siirtyy kontrolleriin B käyttämään VLANia Y. Tällöin alkuperäinen kontrolleri merkitsee asiakkaan tietokantatiedot Anchor-merkinnällä ja uusi kontrolleri merkitsee ne Foreign-merkillä. Asiakkaan tietoliikenne kulkee suoraan kytkettyyn verkkoon uuden tukiaseman ja kontrollerin kautta, mutta asiakkaalle palaava liikenne kulkee alkuperäisen kontrollerin kautta EtherIP-tunnelin läpi uudelle kontrollerilla ja sitä kautta takaisin asiakkaalle. Kuvassa 4 on kuvaannollistettu tämä tapahtuma. (What-when-how 2015.)



Kuva 4: Inter-subnet eli layer 3 roaming (What-when-how 2015)

3 LANGATON LÄHIVERKKO

Langattoman lähiverkon aktiivilaitteita voivat olla reitittimet, kytkimet sekä tukiasemat. Reitittimellä voidaan yhdistää eri verkkoja toisiinsa, esimerkiksi lähiverkko internetiin. Kytkimellä yhdistetään lähiverkon eri laitteet toisiinsa ja tukiasema jakaa internetyhteyden langattomasti lähiverkon käyttäjille.

Ensimmäisiä langattoman verkon tukiasemia kutsuttiin nimityksellä ”fat access point” (fat AP), joka viittaa siihen, että tukiasema oli täysin autonominen: Laite oli itsenäinen kokonaisuus, jolla voitiin luoda pienikokoinen langaton lähiverkko ilman muita laitteita. Jokainen autonominen tukiasema täytyi konfiguroida manuaalisesti, joten suurempia verkkoja varten työ olisi aikaavievää ja hankalaa. Yksittäisiä autonomisia tukiasema sisältävä langaton lähiverkko on stand-alone verkko, koska sen tukiasemat eivät tarvitse muita laitteita toimiakseen. (Sessoms 2015.) (Beal 2015.)

Vastakohtana fat AP:lle oli niin kutsuttu ”thin access point” (thin AP), jota hallinnoidaan WLAN kontrollerilla. Tällöin verkon ylläpitäjän tarvitsee konfiguroida ainoastaan kontrolleria, joka määrittelee siihen liitettyjen tukiasemien toiminnot. Tämä mahdollistaa verkon laajennuksen, koska uudet tukiasemat voi vain kytkeä kontrolleriin eikä niitä tarvitse erikseen konfiguroida. (Sessoms 2015.)

Langaton lähiverkkoa, jota hallinnoidaan kontrollerilla, kutsutaan controller-based WLANiksi ja sen vastakohtana on controller-less WLAN, jonka tukiasemissa itsessään on virtuaalinen kontrolleri. Näin pelkästään tukiasemia sisältävää verkkoa voidaan silti hallinnoida vain yhden laitteen kautta, kuitenkin ilman kontrolleria. (Sessoms 2015.)

3.1 Cisco 2500 WLAN-kontrolleri

Työssä rakennetussa langattomassa lähiverkossa käytetään yhtä Ciscon 2500 sarjan WLAN kontrolleria, johon voidaan liittää 75 tukiasemaa ja näiden kautta voidaan jakaa verkkoyhteys jopa tuhannelle asiakkaalle. Kontrollerin kautta voi kulkea dataliikennettä jopa 1 Gbps:n nopeudella. (Cisco Systems 2014a.)

3.2 Cisco Aironet 3700 tukiasema

Rakennetun lähiverkon tukiasemina käytetään Cisco Aironet 3700 sarjan tukiasemia, jotka voivat käyttää kaikkia 2.4 GHz ja 5 GHz taajuusalueita tarjoten mahdollisimman hyvän kuuluvuuden asiakkaille. (Cisco Systems 2014b.)

Tukiasemissa on sisäiset antennit, joiden horisontaalinen keilanleveys on 360 astetta ja joiden vahvuus on 4 dBi. Sisäisten antennien ansiosta tukiasema on helppo asentaa mihin tahansa, minkä myötä tukiasemat soveltuvat hyvin myös pieniin toimistotiloihin. Laitteeseen on ostettavissa erikseen myös ulkoiset antennit, jotka lisäävät antennien vahvuutta 2 dBi, eli kokonaisvahvuus olisi tällöin 6 dBi. (Cisco Systems 2014b.)

Tukiasemissa on yksi 10/100/1000BASE-T-portti, jolla laitteet voi kytkeä Power over Ethernet -kytkimeen, jolloin erillistä virtajohtoa ei tarvita. Tämän lisäksi laitteessa on yksi konsoliportti, jonka kautta saadaan hallintayhteys laitteeseen. (Cisco Systems 2014b.)

Cisco Aironet 3700 sarjan tukiasemissa on neljä lähettävää ja neljä vastaanottavaa antennia (MIMO-tekniikka), jotka käyttävät tiedonsiirrossa kolmea spatiaalista streamia (Cisco Systems 2014b). Tämän ansiosta tukiasemat voivat lähettää samanaikaisesti kolminkertaisen määrän dataa kuin, jos tukiasemassa olisi vain yksi lähettävä ja vastaanottava antenni (Hucaby 2014, 58).

3.3 Cisco Prime Network Control System

Työssä rakennetun langattoman lähiverkon hallintaohjelmaksi valittiin Cisco Prime Network Control System -ohjelmisto (NCS), jolla voidaan hallita niin langattomia kuin langallisiakin verkkoja. Ohjelmisto tarjoaa verkon ylläpitäjälle yhden työkalun, jolla voidaan esimerkiksi ennustaa radiotaajuuksia, optimoida verkon asetuksia, seurata käyttäjiä heidän laitteesta riippumatta ja monitoroida turvallisuutta. (Cisco Systems 2011a, 1-7).

Cisco Prime NCS on saatavilla niin fyysisessä kuin virtuaalisessa muodossa, mistä jälkimmäinen sopii matalamman vaativuustason käyttöön. Tätä langatonta lähiverkkoa varten on tarkoitus käyttää virtuaalista muotoa, jonka voi ladata Open Virtualization Archive (OVA) -muodossa. Cisco Prime NCS:n virtuaaliselle versiolle on määritetty kolme suositeltua tasoa, joissa eroavat resurssien tarve ja tuettujen laitteiden määrät. Määritellyistä tasoista alhaisin tukisi jopa 4 000 tukiaseman, 1 000 kytkimen ja 240 langattoman LAN kontrollerin käyttöä, joten se riittää hyvin tähän työhön, koska työssä käytetään ainoastaan kahdeksaa tukiasemaa, yhtä kytkintä ja yhtä kontrolleria. (Cisco Systems 2011a, 2-2).

4 JÄRJESTELMIEN KEHITTÄMISEN ELINKAARI

Systems development life cycle (SDLC) eli järjestelmien kehittämisen elinkaari on käsitteellinen malli, joka kuvastaa esimerkiksi tietojärjestelmien tai ohjelmistojen suunnitteluprojektin vaiheita. SDLC:stä on kehitetty useita eri versioita, joista vanhin ja tunnetuin on niin kutsuttu vesiputous-malli. Tässä mallissa vaiheet on peräkkäin ja edellisen tulos on seuraavan vaiheen sisältö ja, kun yhden vaiheen on ohittanut, ei siihen voida enää palata takaisin. Muita SDLC-malleja ovat esimerkiksi suihkulähde, spiraali, v-malli sekä toistava-malli. (Rouse 2015a.) (Tutoriaslpoin 2015.)

Tyypillisimmän järjestelmien kehittämisen elinkaari sisältää seuraavat vaiheet: alustava suunnittelu, rajaaminen, mallisuunnittelu, rakentaminen, testaus ja käyttöönotto (Tutorialspoint 2015). Tämän työn osalta alustava suunnittelu ja rajaaminen piti sisällään laitevaatimusten selvittämisen ja tarvittavan laitemäärän määrittelyn ja nämä vaiheet oli tehty jo ennen työn aloittamista.

4.1 Mallisuunnittelu

Mallisuunnitteluvaiheeseen liittyi tukiasemien sijaintien määrittäminen. Tiedettiin, että tukiasemia on käytettävissä kahdeksan kappaletta sekä se, mitkä kaikki tilat ja alueet haluttiin niillä kattaa. Mallisuunnittelussa selvitettiin tukiasemien kuuluvuuksia ja tutkittiin, onko merkitystä asennetaanko tukiasema huoneen kattoon vai seinään. Kuuluvuustutkinnassa selvisi, ettei ole huomattavaa merkitystä mihin tukiasema sijoitetaan, joten käyttöturvallisuuden takia tukiasemat päätettiin sijoittaa kattoon. Myös alustavien konfigurointien teko ja tarvittavien asetusten ja muiden määritysten tutkiminen kuuluivat mallisuunnitteluun, koska tutkimisen kautta selvitettiin, mitä kaikkia konfigurointeja voisi käyttää.

4.2 Rakentaminen

Rakentamisen vaiheeseen kuului yhden tukiaseman asentaminen väliaikaisesti käyttöön liittämällä se kytkimen kautta kontrolleriin. Myös kontrolleri sekä kytkin

sijoitettiin niille varattuun paikkaan yrityksen SimuNET-labraan. Jatkosuunnitelmana on siirtää kontrolleri ja kytkin yrityksen Cyberlabraan, jossa laitteille voidaan taata katkeamaton virransyöttö, mikä parantaa langattoman lähiverkon toimintaa. Rakennusvaiheessa laitteet myös konfiguroitiin loppuun.

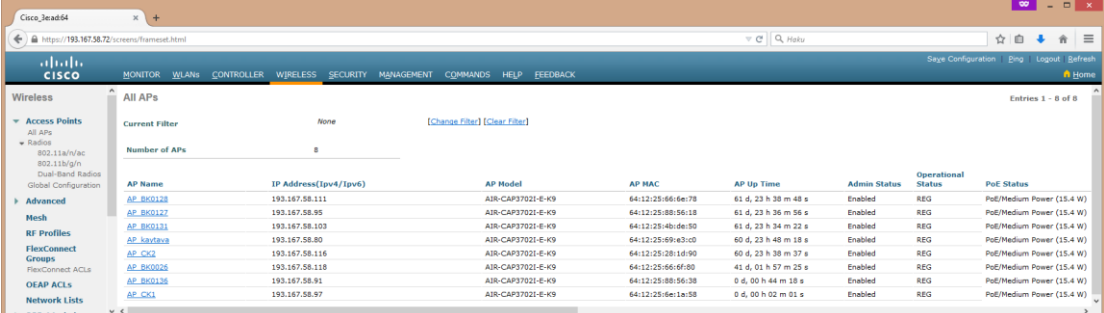
4.3 Testaus

Seuraavassa vaiheessa testattiin kuinka lähiverkko toimi yrittämällä liittyä langattomalla laitteella tukiaseman jakamaan verkkoon. Liittyminen onnistui hyvin ja asiakas sai itselleen IP-osoitteen, minkä myötä hän sai myös yhteyden internettiin.

Testiä laajennettiin liittämällä kaksi muuta tukiasemaa kontrolleriin ja selvitettiin tukiasemien käyttäytyminen asiakkaan siirtyessä laitteensa kanssa nykyisestä tukiasemastaan kauemmas. Kuten oli odotettavissa, asiakas siirrettiin alkuperäisestä tukiasemastaan häntä lähempänä olevaan tukiasemaan, koska näin asiakkaalle pystyttiin tarjoamaan paras mahdollinen yhteys.

4.4 Käyttöönotto

Kun väliaikainen lähiverkko oli testattu toimivaksi, asennettiin kaikki kahdeksan tukiasemaa niille suunniteltuihin paikkoihin ja liitettiin kytkimeen. Tukiasemat nimettiin niiden sijainteihin perustuvilla nimillä, kuvassa 5 on lista kontrolleriin kytketyistä tukiasemista ja niiden tiedoista.



AP Name	IP Address(Ipv4/Ipv6)	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	PoE Status
AP_BKG128	193.167.58.111	AIR-CT5502-K9	64:12:25:66:6e:78	61 d, 23 h 38 m 48 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG127	193.167.58.95	AIR-CT5502-K9	64:12:25:66:6e:18	61 d, 23 h 36 m 56 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG131	193.167.58.103	AIR-CT5502-K9	64:12:25:66:6e:50	61 d, 23 h 34 m 22 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG130	193.167.58.80	AIR-CT5502-K9	64:12:25:66:6e:c0	60 d, 23 h 48 m 18 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG129	193.167.58.116	AIR-CT5502-K9	64:12:25:66:6e:90	60 d, 23 h 38 m 37 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG126	193.167.58.118	AIR-CT5502-K9	64:12:25:66:6e:80	42 d, 01 h 57 m 25 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG125	193.167.58.91	AIR-CT5502-K9	64:12:25:66:6e:38	0 d, 00 h 44 m 18 s	Enabled	REG	PoE/Medium Power (15.4 W)
AP_BKG124	193.167.58.97	AIR-CT5502-K9	64:12:25:66:6e:1a:58	0 d, 00 h 02 m 01 s	Enabled	REG	PoE/Medium Power (15.4 W)

Kuva 5: kontrollerin lista siihen kytketyistä tukiasemista

Myös kytkimeen tehtiin muutoksia ylläpidon parantamiseksi: Tukiasemiin kytkettyihin portteihin lisättiin kuvaukset, joista selviää mihin tukiasemaan kyseinen portti on kytketty.

4.5 Big Bang -malli

Tämän työn edistymistä parhaiten kuvaava SDLC-malli on niin kutsuttu Big Bang, jota käytetään esimerkiksi silloin, kun asiakas itsekään ei tiedä mitä haluaa vaan vaatimukset ja tarpeet selviävät työn ohella. Big Bang -mallia käytetään useimmiten pienissä projekteissa, joilla on pienet työryhmät. (Tutorialspoint 2015.)

Vaikka tässä työssä edistytettiin SDLC:n mukaisissa vaiheissa, ei niiden järjestys ollut täysin virtaviivainen. Esimerkiksi mallisuunnitteluvaiheessa tehdyt kuuluvuuksien mittaukset tehtiin vasta sitten, kun rakennusvaiheen väliaikainen lähiverkko oli jo rakennettu ja testattu toimivaksi. Työssä muutenkin siirryttiin eri vaiheiden välillä hyvin paljon, koska kesken rakentamisen saattoi eteen tulla konfigurointiongelmia, joka piti selvittää ja korjata.

5 TYÖN TOTEUTUS

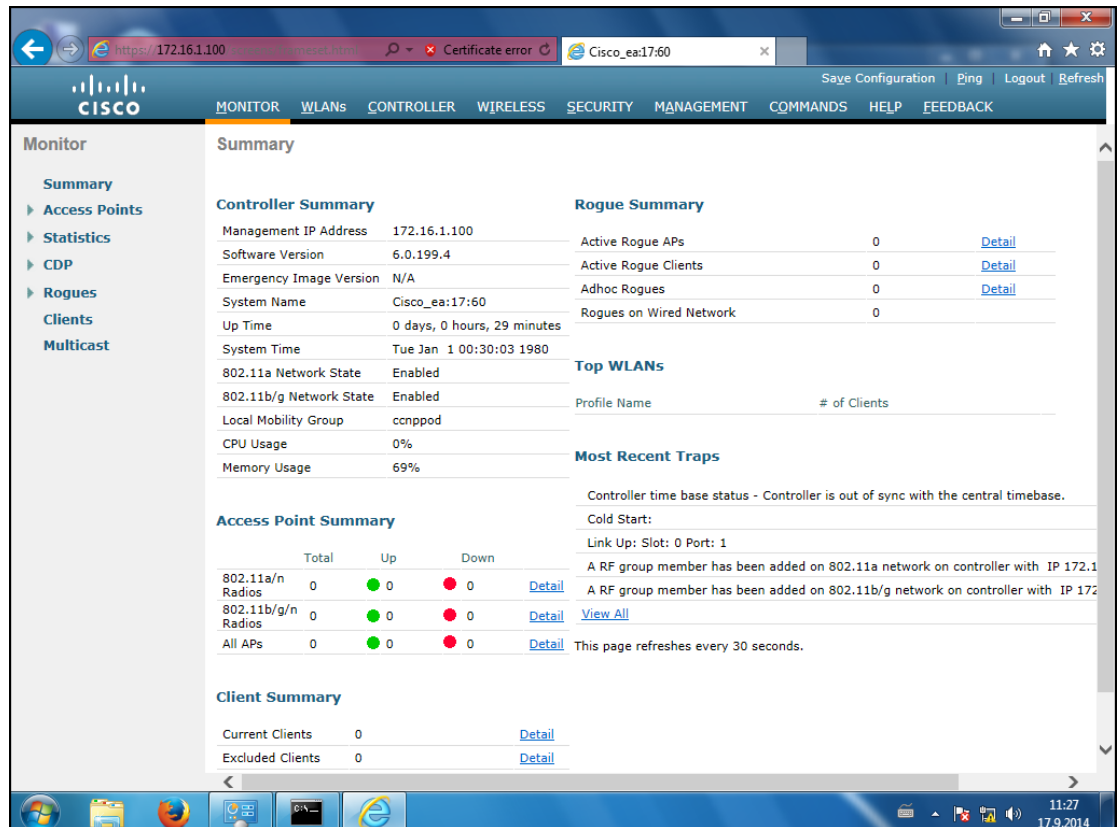
Tämä opinnäytetyö sai alkunsa projektiopinnoista, jotka aloitettiin syyskuussa 2014. Opinnoissa tutustuttiin yrityksen omistuksessa oleviin vanhempiin WLAN-kontrollereihin ja tukiasemiin tekemällä Cisco Academyn tarjoamia harjoituksia, joissa kytkettiin WLAN-kontrollerin sisältävä reititin kahteen tukiasemaan, joiden tulisi jakaa langaton lähiverkko asiakkaille. Näiden harjoitusten jälkeen tutustuttiin uusiin laitteisiin, joista lopulta luotiin uusi langaton lähiverkko yrityksen informaatioteknologian tiloihin.

5.1 Projektiopinnot

Projektiopinnoissa ensimmäisenä tehty harjoitus ei onnistunut, koska tuntemattomasta syystä tukiasemat eivät tarjonneet langatonta verkkoa asiakkaille. Konfiguroinnit tehtiin ohjeiden mukaan eikä laitteissakaan pitänyt olla mitään vikaa, joten syy epäonnistumiseen jäi sillä hetkellä epäselväksi.

Ensimmäisessä harjoituksessa konfiguraatiot tehtiin komentoriviltä suoraan laitteessa, mutta toisessa harjoituksessa yhteys kontrolleriin otettiin nettiselaimen kautta.

Toisessa harjoituksessa saimme yhteyden myös tukiasemiin nettiselaimen kautta, kuvankaappaukset näistä yhteyksistä alla olevissa kuvissa 6 ja 7.



Kuva 6: kontrollerin hallintayhteys nettiselaimen kautta

The screenshot shows the Cisco Aironet 1200 Series Access Point configuration page. The browser address bar shows http://172.16.50.154/ap_event-log.shtml. The page title is "Cisco Aironet 1200 Series Access Point". The hostname is "ap" and the uptime is "10 minutes". The left sidebar contains a menu with options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG (selected), and Configuration Options. The main content area displays the "Event Log" with a table of events. The table has columns for Index, Time, Severity, and Description. The events are listed as follows:

Index	Time	Severity	Description
1	Mar 1 00:00:39.381	Information	Interface BV11 assigned DHCP address 172.16.50.154, mask 255.255.255.0, hostname ap
2	Mar 1 00:00:29.248	Notification	Line protocol on Interface BV11, changed state to up
3	Mar 1 00:00:28.296	Notification	SNMP agent on host ap is undergoing a cold start
4	Mar 1 00:00:28.296	Notification	System restarted --
5	Mar 1 00:00:27.157	Notification	Line protocol on Interface Dot11Radio0, changed state to down
6	Mar 1 00:00:26.157	Notification	Interface Dot11Radio0, changed state to administratively down
7	Mar 1 00:00:08.074	Notification	Line protocol on Interface FastEthernet0, changed state to up
8	Mar 1 00:00:07.074	Error	Interface FastEthernet0, changed state to up
9	Mar 1 00:00:07.072	Information	Logger process started
10	Mar 1 00:00:04.109	Warning	Interface Dot11Radio0, loading the radio firmware (flash:/c1200-k9w7-mx.123-7.JA2/5101.img)
11	Mar 1 00:00:04.108	Notification	Interface Dot11Radio0, changed state to reset

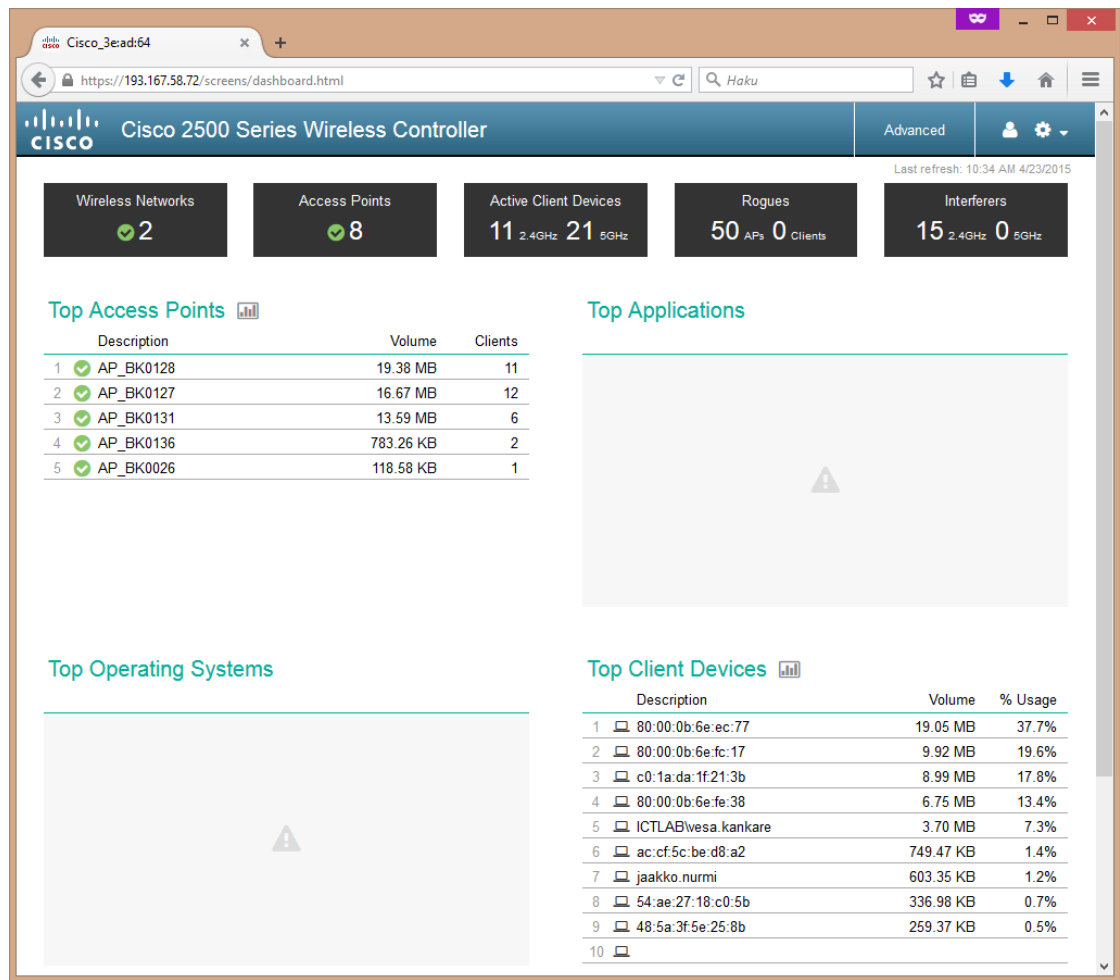
The bottom of the page shows a "Close Window" button and a copyright notice: "Copyright (c) 1992-2005 by Cisco Systems, Inc." The Windows taskbar at the bottom shows the date and time as 12:00 17.9.2014.

Kuva 7: hallintayhteys tukiasemaan nettiselaimen kautta

Toisessakin harjoituksessa ilmeni ongelmia saada langaton lähiverkko toimimaan, kunnes reititin, jossa oli sisäinen kontrolleri, resetoitiin tehdasasetuksiin. Tämän jälkeen tukiasemat saatiin jakamaan langattoman verkkonsa ja asiakas saatiin liitettyä tähän verkkoon.

5.2 Uusi WLAN-kontrolleri

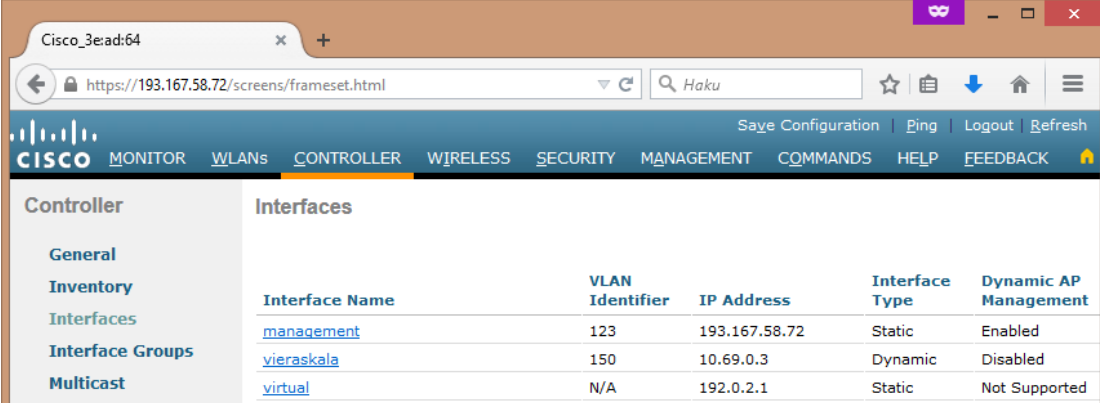
Ennen varsinaisen työn aloittamista kontrollerin osalta, laitteen ohjelmistoversio päivitettiin uusimpaan julkaistuun versioon, joka oli numero 8.0.100.0. Tämän yhtenä uutena ominaisuutena oli optimized roaming, joka parantaa käyttökokemusta sellaisille asiakkaille, jotka pakon edestä kuuluvat heistä kaukana olevaan tukiasemaan tai joilla on vaikeuksia luoda vakaata yhteyttä (Cisco Systems 2015a). Kuvassa 8 on kontrollerin graafisen käyttöliittymän etusivu.



Kuva 8: kontrollerin graafinen käyttöliittymä

5.2.1 Liitännät

WLAN-kontrolleriin konfiguroitiin kolme liitännää, joita käytetään ohjaamaan asiakkaat oikeaan osoitteeseen. Esimerkiksi management-käyttöliittymän kautta tukiasemat sekä pääasialliset asiakkaat saavat yhteyden palomuurin ja siten ne saavat itselleen IP-osoitteen, jotta voivat käyttää internetiä. Vieraskala-käyttöliittymä tarjoaa saman vieraileville asiakkaille ja järjestelmän toimivuuden takia nämä kaksi eri asiakaskuntaa on eroteltu toisistaan. Kuvasta 9 löytyy kontrollerin kolme käyttöliittymää.



Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	123	193.167.58.72	Static	Enabled
vieraskala	150	10.69.0.3	Dynamic	Disabled
virtual	N/A	192.0.2.1	Static	Not Supported

Kuva 9: Kontrollerin kolme käyttöliittymää

Viimeisin käyttöliittymä on nimensä mukaisesti virtuaalinen käyttöliittymä, jonka tärkeimpinä käyttötarkoituksina on toimia DHCP-palvelimen osoitteena ja verkon kautta tapahtuvan autentikoinnin uudelleenlähetysosoitteena. Tässä työssä on erilliset DHCP-palvelimet eikä verkossa tapahtuvaa autentikointia käytetä, joten virtuaalinen käyttöliittymä on tarpeeton. Järjestelmä ei kuitenkaan toimisi tarkoituksenmukaisesti, jos virtuaalista käyttöliittymää ei määritetä tai jos sen määrittää virheellisesti (esimerkiksi käyttää osoitetta 0.0.0.0). Tästä syystä sille täytyy antaa oikea IP-osoite, joka ei saa olla käytössä missään muualla kyseisessä verkossa. (Cisco Systems 2013, 321.)

5.2.2 Eri WLANit asiakkaille ja vierailijoille

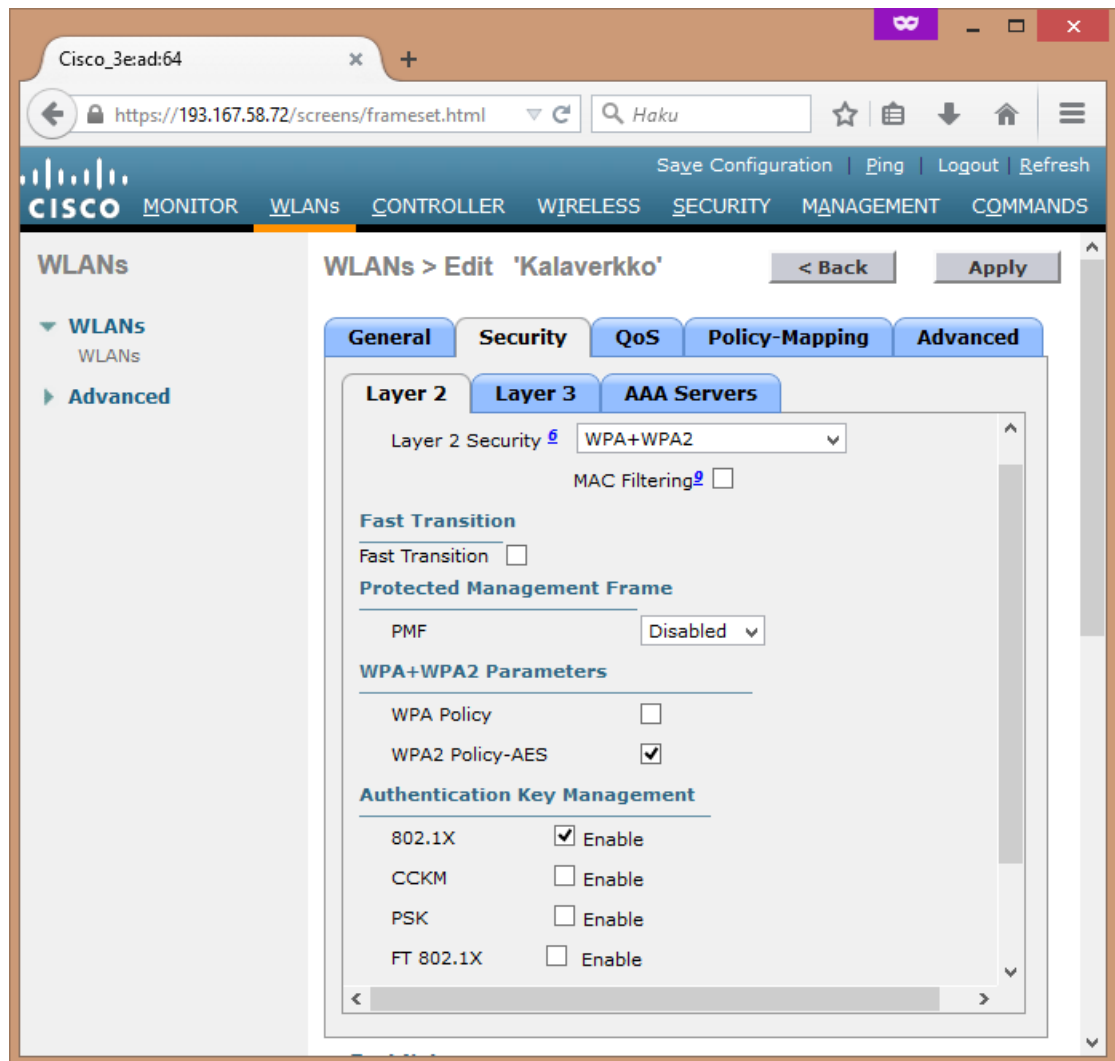
Kontrolleriin luotiin kaksi eri WLANia, Kalaverkko ja Vieraskala. Toinen on tarkoitettu tukiasemille ja pääasiallisille asiakkaille ja toinen vierailijoille. Molemmissa on WPA2-tietoturvatekniikka, joka on tällä hetkellä turvallisin tekniikka langattomalle verkolle. Näissä molemmissa on käytössä AES (engl. Advanced Encryption Standard) salausmenetelmä, jota jopa NSA käyttää tietojensa salaamisessa (Rouse 2015b).

5.2.2.1 WLAN Kalaverkko

Kalaverkossa käytetään dot1x eli 802.1x-standardin mukaista pääsynhallintamenetelmää. Kun asiakas ottaa yhteyden Kalaverkkoon, yhdistetään hänen laitteensa ainoastaan tukiasemaan, josta hän ei vielä saa pääsyä pidemmälle, esimerkiksi internettiin. Asiakkaan täytyy ensin kirjautua tunnuksillaan, jotka jokainen informaatioteknologian opiskelija ja opettaja saa. Asiakkaan antamat tunnukset tarkastetaan erillisellä RADIUS-palvelimella ja hyväksynnän jälkeen, asiakas saa pääsyn koko verkkoon. (Hucaby 2014, 292.) (Smith, Woodhamds & Marg 2010, 96.)

RADIUS-palvelimella käytetään AAA-protokollaa, jonka kautta käyttäjä tunnistautuu käyttöoikeuden saaneeksi käyttäjäksi, hänet valtuutetaan oikeutetuksi käyttämään tai kielletään käyttämästä tiettyjä asioita sekä tilastoidaan käyttäjän tietoja, esimerkiksi kuinka kauan hän oli yhteydessä palvelimeen tai kuinka paljon hän sai tai lähetti dataa yhteyden aikana. (Rouse 2015c.)

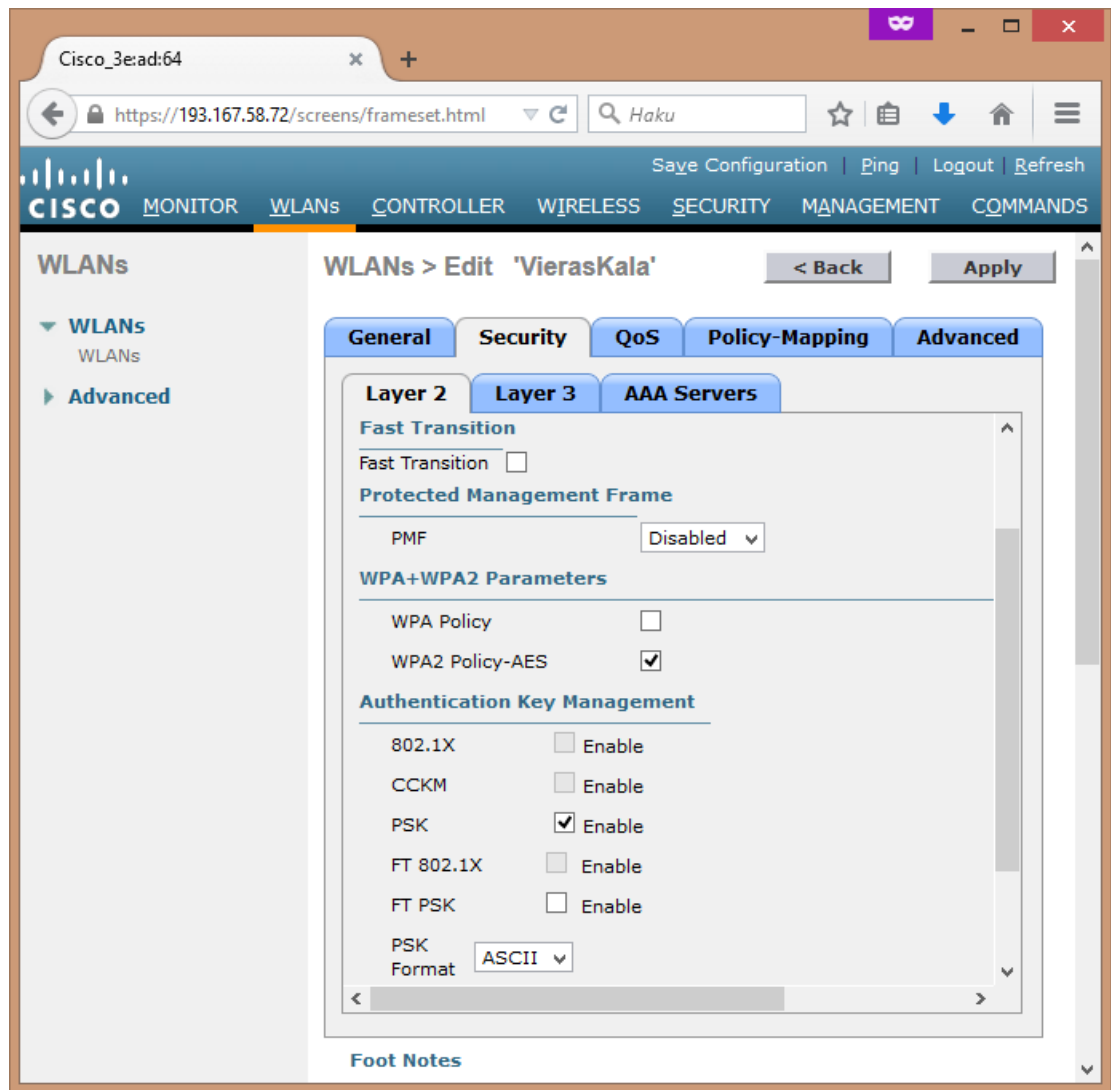
Kuvassa 10 on Kalaverkko-WLANin tietoturvan asetuksista.



Kuva 10: Kalaverkko-WLANin tietoturvan asetukset

5.2.2.2 WLAN Vieraskala

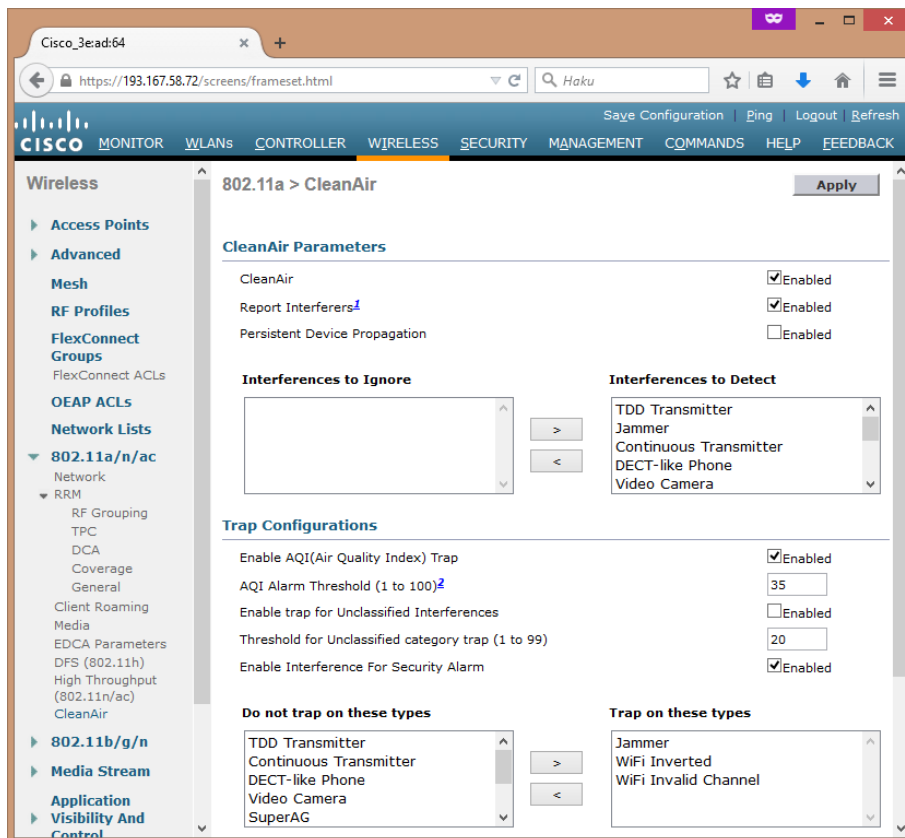
Vieraskalan kirjautumisessa käytetään pre-shared key (PSK) – avaintenjakomenetelmää, joka tarkoittaa sitä, että kyseiselle WLANille on luotu itse määriteltä salasana, joka kerrotaan asiankuuluville henkilöille, jotta he voivat kirjautua tähän WLANiin. Kuvassa 11 on Vieraskala-WLANin salaustekniikan asetukset.



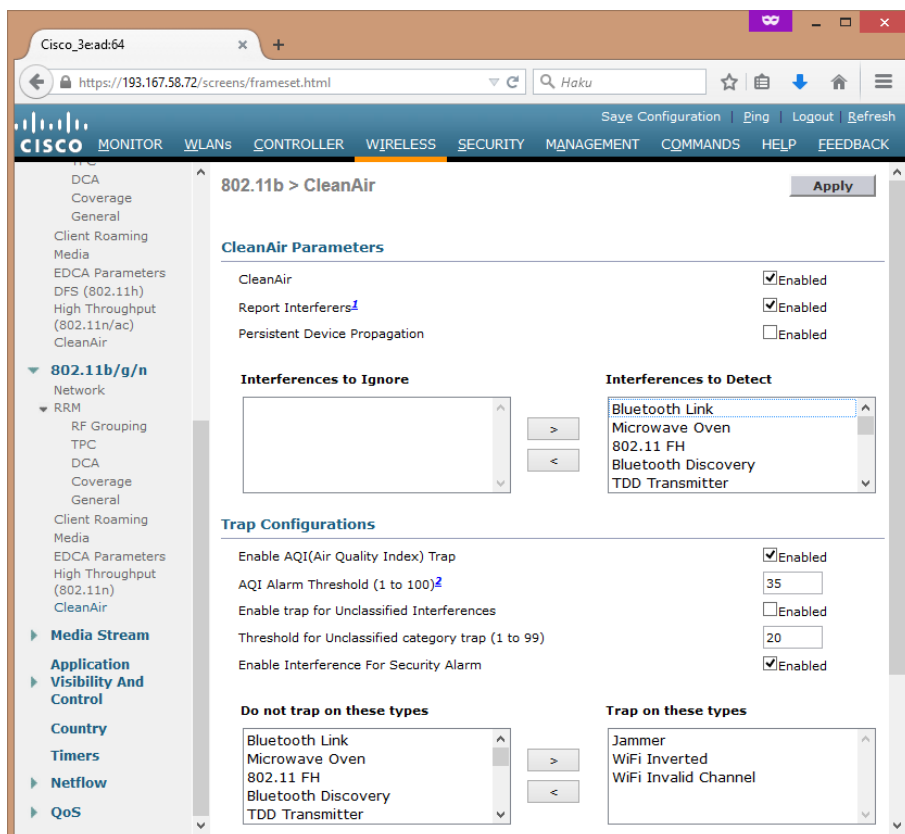
Kuva 11: Vieraskala-WLANin tietoturvan asetukset

5.2.3 CleanAir

Kontrolleriin konfiguroitiin CleanAir, jonka ansiosta langattoman lähiverkon tukiasemat voivat kerätä tietoa kaikista muista laitteista, jotka toimivat samalla taajuusalueella niiden kanssa. Tukiasemat lähettävät tämän tiedon kontrollerille, jonka kautta lähiverkon ylläpitäjä voi ryhtyä toimenpiteisiin korjatakseen tilanteen. Kuvassa 12 on 5 GHz:n taajuuden CleanAir-asetukset ja kuvassa 13 on 2.4 Ghz:n taajuuden asetukset.



Kuva 12: CleanAir-asetukset 5 GHz:n taajuudella



Kuva 13: CleanAir-asetukset 2,4 GHz:n taajuudella

5.3 Langattomat tukiasemat

Työssä rakennettu langaton lähiverkko koostuu yhteensä kahdeksasta Cisco Aironet 3700-sarjan tukiasemasta, jotka asennettiin yrityksen informaatioteknologian osastolle ja sen läheisyyteen. Itse osaston tiloihin asennettiin neljä tukiasemaa, jotta kaikille osastolla työskenteleville asiakkaille voidaan tarjota toimiva ja luotettava langaton lähiverkkoyhteys.

Käyttäjäystävällisyyttä pystyttiin parantamaan sillä, että asennettiin yksi tukiasema osastolle vievälle käytävälle. Näin asiakas saa yhteyden langattomaan lähiverkkoon jo lähestyessään osastoa eikä hän lähtiessäänkään joudu välittömästi pois osaston langattoman lähiverkon kuuluvuusalueelta.

Informaatioteknologian tiloihin kuuluu myös osaston alueelta hieman erillään oleva luokkahuone, johon asennettiin yksi tukiasema. Näin kyseisessä luokassa pidettävillä tunneilla pystyttiin myös käyttämään hyödyksi työssä rakennettua langatonta lähiverkkoa.

Kaksi viimeistä tukiasemaa asennettiin informaatioteknologian osaston läheisyydessä olevaan auditorioon, koska siellä pidetään luentoja suuremmalle ryhmälle ja näillekin haluttiin tarjota langaton lähiverkko.

Tukiasemia ei tarvinnut päivittää tai konfiguroida lainkaan, vaan ne saattoi kytkeä suoraan haluttuun laitteeseen. Testivaiheessa tukiasemat kytkettiin suoraan kontrolleriin, mutta varsinaisessa työssä tukiasemat kytkettiin PoE-kytkimeen, joka oli kytketty kontrolleriin.

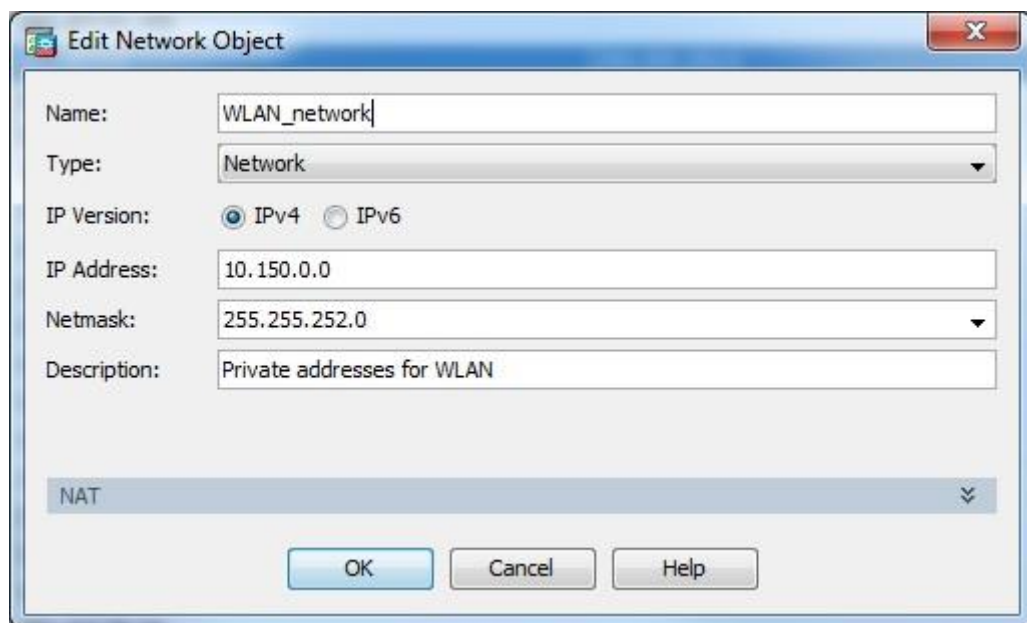
5.4 Power over Ethernet -kytkin

Työhön valittiin Power over Ethernet -kytkin, koska tällöin tukiasemille ei tarvitse erillisiä virtakaapeleita, vaan ne saavat virran suoraan RJ45-kaapelista, jolla ne yhdistetään kytkimeen. Kytkimeen konfiguroitiin käyttäjätunnukset ja tarvittavat salasana sekä telnet- ja ssh-yhteydet. Tämän lisäksi portteihin, joihin tukiasemat kytkettiin, määriteltiin tarvittavat asetukset, jotta asiakkaat ohjataan oikeaan

osoitteeseen. Liitteessä 1 on kytkimen konfiguraatiot, josta IP-osoitteet on muutettu turvallisuussyistä.

5.5 Palomuri

Työssä käytettiin Ciscon 5510-palomuuria, johon konfiguroitiin DHCP-pooli WLAN Vieraskalaa varten VLAN 150 -tunnisteella. DHCP-pooli koostuu 10.150.0.0-osoiteavaruuden yksityisistä osoitteista, joita jaetaan Vieraskala-WLANiin yhdistäville asiakkaille. Kun asiakas haluaa yhteyden internettiin, hänen saamansa yksityinen IP-osoite muutetaan NAT-tekniikalla julkiseksi osoitteeksi. Kuvassa 14 on esitetty palomuriin luotu DHCP-pooli vierailijoita varten. Kuvassa 15 on havainnoillistettu NAT-tekniikan asetukset. DHCP-poolin osoitteet on muutettu tekstiin turvallisuussyistä.



Kuva 14: DHCP-pooli vierailijoita varten

Edit NAT Rule

Match Criteria: Original Packet

Source Interface: Destination Interface:

Source Address: Destination Address:

Service:

Action: Translated Packet

Source NAT Type:

Source Address: Destination Address:

☐ PAT Pool Translated Address:

☐ Round Robin

☐ Extend PAT uniqueness to per destination instead of per interface

☐ Translate TCP and UDP ports into flat range 1024-65535 ☐ Include range 1-1023

☐ Fall through to interface PAT

Options

☒ Enable rule

☐ Translate DNS replies that match this rule

☐ Disable Proxy ARP on egress interface

☐ Lookup route table to locate egress interface

Direction:

Description:

OK Cancel Help

Kuva 15: NAT-asetukset

5.6 Hallintaohjelma Cisco Prime NCS

Tämän työn osalta hallintaohjelman käyttö jäi hyvin vähäiselle, koska ohjelman asennuksessa ilmeni ongelmia ja se saatiin asennettua vasta työn loppuvaiheessa. Ohjelmaan pystyttiin silti tutustumaan sen verran, että siihen saatiin kytkettyä kytkin onnistuneesti sekä kontrolleri alustavasti.

Kuvassa 16 on asetukset, joilla kontrolleri lisättiin ohjelman hallinnan piiriin.

Kytkimen asetukset oli lähes samanlaiset kuin kontrollerissa, ainoat poikkeukset olivat ne, että yhteyden protokollana käytettiin telnettiä kontrollerin SSH-protokollan sijaan ja kytkimessä oli kaksi eri salasanaa, jotka täytyi kertoa hallintaohjelmalle, jotta se voittaa laitteeseen yhteyden.

The screenshot shows the Cisco Prime Network Control System interface. The browser address bar indicates the URL is <https://193.167.58.73/webac>. The page title is "Cisco NCS - Configure Co...". The navigation menu includes Home, Monitor, Configure, Services, Reports, and Administration. The current page is "Add Controllers", with a breadcrumb trail: Configure > Controllers > Add Controllers. The page is divided into three main sections: General Parameters, SNMP Parameters, and Telnet/SSH Parameters. In the General Parameters section, "Add Format Type" is set to "Device Info", "IP Addresses" is "193.167.58.72", and "Wism Auto Add" is unchecked. In the SNMP Parameters section, "Version" is "v2c", "Retries" is "2", "SNMP Timeout" is "10" seconds, and "Community" is masked with dots. In the Telnet/SSH Parameters section, "Protocol" is "SSH", "Username" is "cisco", "Password" and "Confirm Password" are masked with dots, and "Telnet Timeout" is "60" seconds. At the bottom, there are "Add" and "Cancel" buttons. The footer includes "Tools", "Help", "Alarm Browser", and "Alarm Summary" with status indicators.

Cisco Prime Network Control System
Virtual Domain: ROOT-DOMAIN

Home Monitor Configure Services Reports Administration

Add Controllers

Configure > Controllers > Add Controllers

General Parameters

Add Format Type: Device Info

IP Addresses: 193.167.58.72 (comma-separated IP Addresses)

☐ Wism Auto Add

SNMP Parameters

Version: v2c

Retries: 2

SNMP Timeout: 10 (secs)

Community:

Telnet/SSH Parameters

Protocol: SSH

Username: cisco

Password:

Confirm Password:

Telnet Timeout: 60 (secs)

Add Cancel

Tools | Help Alarm Browser | Alarm Summary 0 0 0

Kuva 16: kontrollerin lisääminen hallintaohjelmaan

Kytkimen lisääminen onnistui, mutta kontrollerin lisäämisessä oli jokin tuntematon ongelma, johon ei pystytty vielä paneutumaan. Kytkin löytyi hallintaohjelman Configure-välilehden alta Switches-välilehdeltä. Kuvassa 17 näkyy kaikki asetukset, jotka hallintaohjelma sai kytkimeltä tietoonsa, esimerkiksi kytkimelle annettu nimi ja siinä oleva ohjelmistoversio.

The screenshot shows the Cisco Prime Network Control System (NCS) interface. The browser address bar indicates the URL: <https://193.167.58.73/webacs/loginAction.do?action=login&flashVersi>. The page title is "Cisco NCS - Configure Eth...". The main navigation bar includes "Home", "Monitor", "Configure", "Services", "Reports", and "Administration". The "Configure" menu is expanded, showing "System", "Switches", and "Services". The "System" menu is selected, and the "Summary" page is displayed. The page shows the configuration for a switch named "mustekala" with IP Address "193.167.58.248". The software version is "12.2(55)SE1". The location is "mustekala". The last inventory collection date is "2015-Apr-20, 13:14:08 UTC". The inventory collection status is "Managed and partially synchronized". The reachability status is "Reachable". The SNMP Parameters section shows Version "v2c", Retries "2", Timeout "10 (secs)", and Community "*****". The Telnet/SSH Parameters section shows Protocol "SSH", Username "cisco", Password "*****", Confirm Password "*****", Enable Password "*****", Confirm Password "*****", and Timeout "60 (secs)". The page has "Reset", "Save", and "Cancel" buttons at the bottom.

Kuva 17: kytkimen asetukset onnistuneen lisäyksen jälkeen

Kontrollerissa voi jaotella kaikki sen löytämät tukisemat ystävällisiin ja pahansuopaisiin, minkä lisäksi ne voi kategorisoida sisäisiin ja ulkoisiin. Yrityksen tiloissa toimii toinenkin langaton lähiverkko ja tämän tukiasemat jaoteltiin ystävällisiin sisäisiin tukiasemiin, koska niiden mahdollisesti häiriötäkin aiheuttava toiminto on hyväksyttävää. Kuvassa 17 on listattu ystävälliset tukiasemat. Kuvassa 18 on listattu kategorisoimattomat tukiasemat, joiden jaottelu oikeaan ryhmään on vielä kesken.

Cisco_3ead64

https://193.167.58.72/screens/frameset.html

Save Configuration | Ping | Logout | Refresh

CISCO

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Home

Monitor

Summary

- Access Points
- Cisco CleanAir
- Statistics
- CDP
 - Interface Neighbors
 - AP Neighbors
 - Traffic Metrics
- Rogues
 - Friendly APs
 - Malicious APs
 - Custom APs
 - Unclassified APs
 - Rogue Clients
 - Adhoc Rogues
 - Rogue AP ignore-list
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling

Friendly Rogue APs

Entries 1 - 23 of 23

Current Filter: None [Change Filter] [Clear Filter]

Remove

<input type="checkbox"/>	MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status	
<input type="checkbox"/>	98:4b:e1:2a:03:63	KYAMK	36	1	0	Internal	▼
<input type="checkbox"/>	98:4b:e1:2a:03:64	KYAMK visitor	Unknown	0	0	Internal	▼
<input type="checkbox"/>	98:4b:e1:2a:03:73	KYAMK	1	6	1	Internal	▼
<input type="checkbox"/>	98:4b:e1:2a:03:74	KYAMK visitor	1	6	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:5e:b1	KYAMK	Unknown	0	1	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:5e:b2	KYAMK visitor	5	3	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:9e:81	KYAMK	Unknown	0	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:9e:82	KYAMK visitor	100	2	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:ee:c1	KYAMK	Unknown	0	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:ee:c2	KYAMK visitor	Unknown	0	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:ee:d1	KYAMK	5	4	0	Internal	▼
<input type="checkbox"/>	a0:48:1c:3c:ee:d2	KYAMK visitor	Unknown	0	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:49:ed:03	KYAMK	132	2	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:49:ed:04	KYAMK visitor	132	2	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:49:ed:13	KYAMK	5	2	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:49:ed:14	KYAMK visitor	Unknown	0	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:10:72	KYAMK visitor	5	1	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:20:21	KYAMK	100	1	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:20:22	KYAMK visitor	100	1	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:20:30	Unknown	1	4	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:20:31	KYAMK	1	4	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:20:32	KYAMK visitor	1	5	0	Internal	▼
<input type="checkbox"/>	d8:9d:67:4a:50:32	KYAMK visitor	Unknown	0	0	Internal	▼

Kuva 18: ystävälliset tukiasemat

Cisco_3ead64

https://193.167.58.72/screens/frameset.html

Save Configuration | Ping | Logout | Refresh

CISCO

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Home

Monitor

Summary

- Access Points
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
- Cisco CleanAir
- Statistics
- CDP
- Rogues
 - Friendly APs
 - Malicious APs
 - Custom APs
 - Unclassified APs
 - Rogue Clients
 - Adhoc Rogues
 - Friendly Adhoc
 - Malicious Adhoc
 - Custom Adhoc
 - Unclassified Adhoc
 - Rogue AP ignore-list
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling

Unclassified Rogue APs

Entries 1 - 17 of 17

Current Filter: None [Change Filter] [Clear Filter]

Remove

Contain

Move to Alert

<input type="checkbox"/>	MAC Address	SSID	Channel	# Detecting Radios	Number of Clients	Status	
<input type="checkbox"/>	20:62:74:34:e7:fa	NOKIA Lumia 930_6949	11	3	0	Alert	▼
<input type="checkbox"/>	70:73:cb:b6:30:99	Apple Time Capsule	1	5	0	Alert	▼
<input type="checkbox"/>	70:73:cb:b6:30:9a	Apple Time Capsule	100	3	0	Alert	▼
<input type="checkbox"/>	98:4b:e1:2a:03:60	Unknown	36	2	0	Alert	▼
<input type="checkbox"/>	98:4b:e1:2a:03:70	Unknown	1	7	0	Alert	▼
<input type="checkbox"/>	a0:48:1c:3c:9e:80	Unknown	100	2	0	Alert	▼
<input type="checkbox"/>	a0:48:1c:3c:ee:c0	Unknown	44	1	0	Alert	▼
<input type="checkbox"/>	b0:b2:dc:6a:27:75	KyamkVITALS	1	2	0	Alert	▼
<input type="checkbox"/>	b0:b2:dc:6a:57:19	KyamkVITALS	11	3	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:49:ed:00	Unknown	132	2	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:49:ed:10	Unknown	5	2	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:49:ee:50	Unknown	13	1	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:4a:20:20	Unknown	100	1	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:4a:50:20	Unknown	108	1	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:4a:50:30	Unknown	5	1	0	Alert	▼
<input type="checkbox"/>	d8:9d:67:4a:50:90	Unknown	1	1	0	Alert	▼
<input type="checkbox"/>	e8:40:f2:16:1b:cf	f34747	6	5	0	Alert	▼

Kuva 19: kategorisoimattomat tukiasemat

6 LOPPUPÄÄTELMÄT

Työ eteni vaihtelevasti, koska alussa meni paljon aikaa tutustua laitteisiin ja tutkia niiden ominaisuuksia sekä opetella niiden käyttämistä. Alussa työtä kuitenkin oli tekemässä kolmekin henkilöä, mikä nopeutti ja helpotti suunnittelua, kun oli useampi henkilö vaikuttamassa. Loppuvaiheessa aikaa oli rajallisesti ja työ eteni vain yhden ihmisen voimin, minkä lisäksi oli ongelmia hallintaohjelman asennuksen kanssa. Lopulta kuitenkin päätettiin jättää hallintaohjelman osuus opinnäytetyöstä kokonaan pois, joten työ pystyttiin saattamaan loppuun.

Työssä rakennettu langaton lähiverkko on perusrakenteeltaan valmis ja käyttökuntoinen, mutta se vaatii vielä hienosäätöä. Esimerkiksi palomuurin konfiguraatiot ovat hyvin monimutkaisia ja pienikin virheellinen muutos saattaa aiheuttaa sen, ettei asiakas pysty kirjautumaan Kalaverkkoon. Palomuurin konfigurointi ei kuitenkaan kuulunut tämän työn piiriin, joten sen puutteisiin ei pystytty puuttumaan.

Yhtenä jatkokehityksenä on ehdottomasti hallintaohjelman käyttöönotto ja sen kautta langattoman lähiverkon hallinnan parantaminen. Myös tutustuminen kontrollerin monipuolisiin asetuksiin on kehityskelpoinen asia, koska siten verkon toimintaa pystytään parantamaan.

LÄHTEET

Beal, V. 2015. What is Stand-Alone? Verkkojulkaisu. Saatavissa:

http://www.webopedia.com/TERM/S/stand_alone.html [viitattu 14.4.2015]

Cisco System. 2009a. Key Performance Benefits of 802.11n. Verkkojulkaisu.

Saatavissa: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11n/white_paper_c11-513840.pdf [viitattu 23.1.2015].

Cisco Systems. 2009b. Cisco ClientLink: Optimized Device Performance with 802.11n. Verkkojulkaisu. Saatavissa:

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/white_paper_c11-516389.pdf [viitattu 21.4.2015].

Cisco Systems. 2011. Cisco Prime Network Control System Configuration Guide.

Verkkojulkaisu. Saatavissa: <http://www.cisco.com/c/en/us/td/docs/wireless/ncs/1-0/configuration/guide/NCS10cg.pdf> [viitattu 24.2.2015]

Cisco Systems. 2013. Cisco Wireless LAN Controller Configuration Guide, Release 7.4. Verkkojulkaisu. Saatavissa:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED.pdf [viitattu 20.4.2015]

Cisco Systems. 2014a. Cisco 2500 Series Wireless Controller Data Sheet.

Verkkojulkaisu. Saatavissa:

http://www.cisco.com/c/en/us/products/collateral/wireless/2500-series-wireless-controllers/data_sheet_c78-645111.pdf [viitattu 22.1.2015].

Cisco Systems. 2014b. Cisco Aironet 3700 Series Access Point Data Sheet.

Verkkojulkaisu. Saatavissa:

http://www.cisco.com/c/en/us/products/collateral/wireless/3700-series-access-point/data_sheet_c78-729421.pdf [viitattu 20.2.2015]

Cisco Systems. 2015. Release Notes for Cisco Wireless LAN Controllers and

Lightweight Access Points for Release 8.0.100.0. Verkkojulkaisu. Saatavissa:

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn80.html>

[viitattu 11.3.2015]

Geier, J. 2010. WLAN Design: Range, Performance, and Roaming Considerations.

Verkkojulkaisu. Saatavissa:

<http://www.ciscopress.com/articles/article.asp?p=1613796&seqNum=4> [viitattu

22.4.2015]

Grandlund, K. 2007. Tietoliikenne. Jyväskylä: WSOYpro/Docendo-tuotteet

Hucaby, D. 2014. CCNA Wireless 640-722 Official Cert Guide. Yhdysvallat: Cisco Press.

Kelly, V. 2015. New IEEE 802.11ac™ Specification Driven by Evolving Market Need for Higher, Multi-User Throughput in Wireless LANs. Verkkojulkaisu.

Saatavissa: http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html [viitattu

26.3.2015]

KyAMK Informaatioteknologia. 2015a. KyAMK Informaatioteknologia.

Verkkojulkaisu. Saatavissa:

[http://www.ictlab.kyamk.fi/index.php/fi/informaatioteknologia/etusivu/48-](http://www.ictlab.kyamk.fi/index.php/fi/informaatioteknologia/etusivu/48-suomeksi/informaatioteknologia/169-kyamk-informaatioteknologia)

[suomeksi/informaatioteknologia/169-kyamk-informaatioteknologia](http://www.ictlab.kyamk.fi/index.php/fi/informaatioteknologia/etusivu/48-suomeksi/informaatioteknologia/169-kyamk-informaatioteknologia) [viitattu

26.3.2015]

KyAMK Informaatioteknologia. 2015b. Tietoverkkotekniikka. Verkkojulkaisu.

Saatavissa:

<http://ictlab.kyamk.fi/index.php/fi/tietoverkkotekniikka/etusivu/oppimisymparisto>

[viitattu 9.3.2015]

KyAMK Informaatioteknologia. 2015c. Kyberturvallisuus. Verkkojulkaisu.

Saatavissa: <http://www.ictlab.kyamk.fi/index.php/fi/kyberturvallisuus/etusivu> [viitattu

26.3.2015]

KyAMK Informaatioteknologia. 2015d. Peliohjelmointi. Verkkojulkaisu. Saatavissa:

<http://ictlab.kyamk.fi/index.php/fi/peliohjelmointi/etusivu> [viitattu 9.3.2015]

Kymenlaakson ammattikorkeakoulu. 2014. Kyamk. Verkkojulkaisu. Saatavissa: <http://www.kyamk.fi/Kyamk/> [viitattu 9.3.2015]

Kymenlaakson ammattikorkeakoulu. 2015. Koulutustarjonta. Verkkojulkaisu. Saatavissa: www.kyamk.fi/Hakijalle/Koulutustarjonta/ [viitattu 9.3.2015]

Liang, D., Hao, L. & Heath, R.W. 2002. Multiple-input multiple-output wireless communication systems using antenna pattern diversity. Verkkojulkaisu. Saatavissa: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1188227&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D1188227 [viitattu 23.1.2015].

Mitchell, B. 2015. Wireless Standards 802.11a, 802.11b/g/n, and 802.11ac. Verkkojulkaisu. Saatavissa: <http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm> [viitattu 8.4.2015]

Penttinen, J. 2006. Tietoliikennetekniikka. Helsinki: Werner Söderström Osakeyhtiö

Puska, M. 2005. Langatomat lähiverkot. Helsinki: Talentum

Rohde & Schwarz GmbH & Co. KG. 2015. Assessing a MIMO Channel. Verkkojulkaisu. Saatavissa: http://cdn.rohde-schwarz.com/pws/dl_downloads/dl_application/application_notes/1sp18/1SP18_10e.pdf [viitattu 26.4.2015]

Rouse, M. 2015a. Systems development life cycle (SDLC). Verkkojulkaisu. Saatavissa: <http://searchsoftwarequality.techtarget.com/definition/systems-development-life-cycle> [viitattu 8.4.2015]

Rouse, M. 2015b. What is Advanced Encryption Standard (AES)?. Verkkojulkaisu. Saatavissa: <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard> [viitattu 20.4.2015]

Rouse, M. 2015c. What is authentication, authorization, and accounting (AAA)?. Verkkojulkaisu. Saatavissa:

<http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting> [viitattu 20.4.2015]

Rube, T. 2015. High Performance LAN (Hiperlan). Verkkojulkaisu. Saatavissa: <http://www.wirelesscommunication.nl/reference/chaptr01/wrlslans/hiperlan.htm> [viitattu 8.4.2015]

Sessoms, D. 2015. Controller vs. Controllerless Wifi: What's the Difference?. Verkkojulkaisu. Saatavissa: <http://www.securedgenetworks.com/mobility-blog/Controller-vs-Controllerless-Wifi-Whats-the-Difference> [viitattu 14.4.2015]

Smith, J., Woodhamds, J. & Marg, R. 2010. Controlled-Based Wireless LAN Fundamentals. Yhdysvallat: Cisco Press.

Tutorialspoint. 2015. Software Development Life Cycle (SDLC). Verkkojulkaisu. Saatavissa: http://www.tutorialspoint.com/sdlc/sdlc_tutorial.pdf [viitattu 8.4.2015]

Webopedia. 2015a. 802.11 IEEE wireless LAN Standards. Verkkojulkaisu. Saatavissa: http://www.webopedia.com/TERM/8/802_11.html [viitattu 8.5.4.2015]

What-when-how. 2015. Client Roaming/Mobility Events (Cisco Wireless LAN Controllers). Verkkojulkaisu. Saatavissa: <http://what-when-how.com/deploying-and-troubleshooting-cisco-wireless-lan-controllers/client-roamingmobility-events-cisco-wireless-lan-controllers/> [viitattu 22.4.2015]

Wi-Fi Alliance. 2015. Certification. Verkkojulkaisu. Saatavissa: <http://www.wi-fi.org/certification> [viitattu 8.4.2015]

KYTKIMEN KONFIGURAATIOT

Current configuration : 3045 bytes

version 12.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname mustekala

boot-start-marker

boot-end-marker

enable secret 5 \$1\$x15u\$ERHpb3EhiZnYEte29v82Q/

username cisco password 7 1235104719000D

no aaa new-model

system mtu routing 1500

vtp mode transparent

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

vlan 99

name Management

vlan 100

name Kamerate

KYTKIMEN KONFIGURAATIOT

```
vlan 123  
name Vieraat
```

```
vlan 150  
name WLAN
```

```
interface FastEthernet0/1  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/2  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/3  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/4  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/5  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/6  
switchport access vlan 100  
switchport mode access
```

```
interface FastEthernet0/7
```

KYTKIMEN KONFIGURAATIOT

```
shutdown
```

```
interface FastEthernet0/8
```

```
shutdown
```

```
interface FastEthernet0/9
```

```
shutdown
```

```
interface FastEthernet0/10
```

```
shutdown
```

```
interface FastEthernet0/11
```

```
shutdown
```

```
interface FastEthernet0/12
```

```
shutdown
```

```
interface FastEthernet0/13
```

```
description Linkki AP:lle BK0127:ssa
```

```
switchport access vlan 123
```

```
switchport mode access
```

```
interface FastEthernet0/14
```

```
description Linkki AP:lle BK0136:ssa
```

```
switchport access vlan 123
```

```
switchport mode access
```

```
interface FastEthernet0/15
```

```
description Linkki AP:lle BK0128:ssa
```

```
switchport access vlan 123
```

```
switchport mode access
```

KYTKIMEN KONFIGURAATIOT

```
interface FastEthernet0/16
description Linkki AP:lle BK0131:ssa
switchport access vlan 123
switchport mode access
```

```
interface FastEthernet0/17
description Linkki AP:lle Kaytavassa
switchport access vlan 123
switchport mode access
```

```
interface FastEthernet0/18
description Linkki AP:lle BK0026:ssa
switchport access vlan 123
switchport mode access
```

```
interface FastEthernet0/19
description Linkki AP:lle CK0074:ssa (ovi)
switchport access vlan 123
switchport mode access
```

```
interface FastEthernet0/20
description Linkki AP:lle CK0074:ssa (taka)
switchport access vlan 123
switchport mode access
```

```
interface FastEthernet0/21
shutdown
```

```
interface FastEthernet0/22
shutdown
```

KYTKIMEN KONFIGURAATIO

```
interface FastEthernet0/23
```

```
shutdown
```

```
interface FastEthernet0/24
```

```
shutdown
```

```
interface GigabitEthernet0/1
```

```
description Trunkki Lohikyttimeen
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
interface GigabitEthernet0/2
```

```
description Trunkki Controlleriin
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
interface Vlan1
```

```
no ip address
```

```
interface Vlan99
```

```
ip address 193.167.58.248 255.255.255.240
```

```
ip default-gateway 193.167.58.241
```

```
ip classless
```

```
ip http server
```

```
ip http secure-server
```

```
ip sla enable reaction-alerts
```

```
snmp-server community public RO
```

```
snmp-server community private RW
```

KYTKIMEN KONFIGURAATIOT

```
line con 0
logging synchronous
line vty 0 4
logging synchronous
login local
line vty 5 15
login
```